Case/383604

SERVICES CONTRACT

-between-

(1) THE SCOTTISH MINISTERS (THE "PURCHASER")

-and-

(2) PEOPLEPLUS GROUP LIMITED (THE "SERVICE PROVIDER")

-relating to the supply of-

FAIR START SCOTLAND EMPLOYABILITY SUPPORT SERVICES 2018 – LOT 1 - GLASGOW

Table of Contents

SECTION A INTRODUCTORY PROVISIONS

1. Definitions and Interpretation
2. Condition Precedent
3. Nature of the Contract
4. Period
5. Break
5A. Implementation
6. Specification and Service Levels
7. Pricing Schedule
8. Management Arrangements

SECTION B MISCELLANEOUS PROVISIONS INCLUDING THOSE RELATING TO PRICE, PAYMENT AND INFORMATION

9. Service Provider's Status
10. Notices
11. Price
12. Payment and Invoicing
13. Recovery of Sums Due
14. Data Protection Act
15. Freedom of Information
16. Purchaser Protected Information
17. Service Provider Sensitive Information
18. Audit and Records Management
19. Publicity

SECTION C PROVISION OF SERVICES

20. Provision of the Services
21. Deliverables and Milestones
21A. Assurance and Fraud Reviews

SECTION D STAFF INVOLVED IN THE PROVISION OF SERVICES

22. Key Individuals
23. Offers of Employment
24. Staff transfer at commencement
25. Information about Service Provider Employees
26. Staff transfer on expiry or termination
27. Security

SECTION E PROVISIONS RELATING TO INTELLECTUAL PROPERTY AND GOVERNANCE

28. Parties' pre-existing Intellectual Property Rights
29. Specially Created Intellectual Property Rights
30. Licenses of Intellectual Property Rights
31. Claims relating to Intellectual Property Rights
32. Assignation
33. Change of Control
34. Sub-Contracting
35. Amendment

SECTION F SERVICE PROVIDER CONDUCT REQUIREMENTS

36. Compliance with the Law etc.
37. Official Secrets Acts
38. Service Provider's responsibility for staff etc.
39. Access to the Purchaser's premises
40. Service Provider's Equipment
41. Purchaser Property
42. Health and Safety etc.
42A. Effective Procedures
43. Offences
44. Tax arrangements
45. Discrimination
46. Blacklisting
47. Sustainability etc.
48. Conflicts of Interest

SECTION G FINAL PROVISIONS

49. Warranties and Representations
50. General Indemnity
51. Limitation of Liability
52. Insurances
53. Force Majeure
54. Dispute Resolution
55. Severability
56. Waiver and Cumulative Remedies
57. Termination Rights
58. Termination on Insolvency or Change of Control
59. Exit Management
60. Consequences of Expiry or Termination
61. Entire Agreement
62. Governing Law and Jurisdiction

SCHEDULES

Schedule 1	Specification and Service Levels
Schedule 2	Pricing Schedule
Schedule 3	Change Control Procedures
Schedule 4	Management Arrangements
Schedule 5	Key Individuals
Schedule 6	Approved Sub-contractors
Schedule 7	Service Provider Sensitive Information
Schedule 8	Parent Company Guarantee – NOT USED
Schedule 9	Model Contract regarding Data Protection Directive 95/46/EC
Schedule 10	Exit Management
Schedule 11	Business Continuity and Disaster Recovery (BCDR)
Schedule 12	Security
Schedule 13	Implementation Plan

PREAMBLE:

ONE The Purchaser requires the provision of services;

TWO On 9th March 2017 the Purchaser's contract notice relating to the Services was published in the Official Journal of the European Union with reference number 2017/S 048-088157;

THREE Not Used;

FOUR On 9 March 2017 the Purchaser issued its ITT to potential Service Providers (including the Service Provider) in respect of the provision of services;

FIVE On 23rd May 2017 the Service Provider submitted its Tender;

SIX On the basis of the Tender, the Purchaser has selected the Service Provider to supply the Services under the Contract;

SEVEN The Contract establishes standard terms of supply for the provision of services;

EIGHT The Contract also includes:

- a Specification setting out the Services that the Service Provider has undertaken to provide including Service Levels setting out particular levels of service that the Service Provider has undertaken to meet;
- a Pricing Schedule setting out details of the pricing of the Services, including provision for Service Credits;
- details of Key Individuals involved in the provision of the Services;
- details of approved sub-contractors as at Contract award;
- details of the Service Provider's information which is deemed to be Service Provider Sensitive Information;
- Management Arrangements for the strategic management of the relationship between the Parties.

SUBSTANTIVE PROVISIONS:

SECTION A: INTRODUCTORY PROVISIONS

1. Definitions and Interpretation

1.1. In the Contract, unless the context otherwise requires, the following terms have the meanings given to them below:

"Access to Work (AtW)" Access to Work is a Department for Work and Pensions service that provides practical advice and support to disabled people and their employers to help overcome work related obstacles resulting from disability. The service also provides grants towards additional work-related support relating to a person's disability.

"**Achieve**" or "**Achievement**" means meeting the criteria for the achievement or satisfaction of a Milestone, as set out in the Implementation Plan.

"**Approval**" means the written consent of the Purchaser.

"**Assignee**" has the meaning given in clause 32.2 (Assignation).

"Balance of time" means the remaining period that a Customer can expect to receive pre-employment and in-work support should they disengage from the Service.

"Baseline Personnel Security Standard" means the pre-employment controls for all civil servants, members of the Armed Forces, temporary staff and government contractors generally.

"BCDR Plan" means the business continuity and disaster recovery plan set out in Schedule 11 (Business Continuity and Disaster Recovery (BCDR)), as may be amended from time to time.

"Better off in Work Calculation" means a better off calculation that produces accurate estimates of how much better off a Customer could be in work based on information supplied by the Customer, of potential in-work benefits and tax credits.

"Branding" means all names, logos, images, designs and marks of the Purchaser associated with the Programme and the relevant website domain names including, without limitation, those domain names listed in Schedule 1 (Specification and Service Levels).

"Case Conferencing" means a formal, planned, and structured event separate from regular contacts. The goal of case conferencing is to provide holistic, coordinated, and integrated services across organisations, and to reduce duplication, to best support the Customer.

"Change" means as defined in paragraph 1.1 of Schedule 3 (Change Control Procedures).

"Change Control Notice" or "CCN" a written response or request made by either the Service Provider or the Purchaser in accordance with the Change Control Procedure,

"Change Control Procedures" means the change control procedure specified in Schedule 3 – Change Control Procedures.

"**Change in Law**" means any change in Law which impacts on the performance of the Services which comes into force after the Effective Date.

"Community Benefits" means benefits for society or the environment.

"Continuous Improvement Strategy" means a strategy for improving the provision of

the Services which is produced by the Service Provider.

"**Contract**" means this Contract between the Parties consisting of clauses and thirteen Schedules.

"Contract Charges" means the prices (inclusive of any Milestone Payments, licence costs, support and maintenance costs, exclusive of any applicable VAT), payable to the Service Provider by the Purchaser under this Contract, as set out in the Pricing Schedule, for the full and proper performance by the Service Provider of its obligations under this Contract.

"Contract Period" means the term of the Contract as defined in clause 4.1 provided that such term shall be extended where applicable in accordance with clause 4.2 and shall also include any additional periods of time as required in respect of clauses 4.3 (if applicable) and 4.4 (if applicable) (subject to any earlier date where the Contract is terminated in accordance with the terms of the Contract).

"Contract Review Report" refers to a monthly report on service delivery performance, at a Lot level highlighting issues, risks and best practice.

"Contract Year" shall mean the 12 month period commencing on the Effective Date or any anniversary thereof.

"**Contracting Authority**" has the meaning given in regulation 2 of the Public Contracts (Scotland) Regulations 2015;

"**Control**" has the meaning given in section 450 of the Corporation Tax Act 2010.

"**Core Hours**" means an hour between 0900 hours and 1700 hours on a Working Day.

"Customer" means any individual to whom the Service Provider provides support pursuant to the Contract.

"Customer Charter" means the document which details the Service Provider's values and principles and which includes a description of the guaranteed standards of service to be provided to Customers, how the Services will be delivered to those Customers and what the expected outcomes are from a Customer's perspective.

"Data Sharing Protocol" means the data sharing protocol entered into between the Service Provider and the Purchaser with relevant third parties in relation to the Services (e.g. the Department for Work and Pensions, and/or the Partner Organisations) annexed to Schedule 9 (Model Contract regarding Data Protection Directive 95/46/EC).

"**Default**" means any breach of the obligations of a Party under the Contract (including material breach) or any negligent act, omission or statement of a Party in connection with or in relation to the Contract.

"Delay" means:

(a) a delay in the Achievement of a Milestone by its Milestone Date; or

(b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;

"**Deliverable**" means an item, feature or service associated with the provision of the Services which is required to be delivered by the Service Provider at a Milestone Date or at any other stage during the performance of the Contract.

"**Detailed Implementation Plan**" means the detailed plan for the implementation of the

Services which is developed in accordance with paragraph 41 (Mobilisation and Implementation) Schedule 1 (Specification and Service Levels).

"Disabled Customers" means people defined as disabled by the Equalities Act 2010 and in need of the specialist support that is only available in the Intense or Advanced strands of the Scottish Employability Programme.

"Documentation" means all documentation as:

(a) is required to be supplied by the Service Provider to the Purchaser under this Contract;

(b) would reasonably be required by a competent third party contracted by the Purchaser to provide the Services in accordance with Good Industry Practice;

(c) is required by the Service Provider in order to provide the Services; and/or

(d) has or will be generated for the purpose of providing the Services.

"Effective Date" means the date which this Contract is signed by both Parties. (October 2017)

"Employment and Support Allowance" (ESA) means the integrated contributory and income-based benefit, which replaced Incapacity Benefit and Income Support, paid on the grounds of incapacity for most new and repeat customers from October 2008. ESA is paid to those who have limited capability for work (i.e. the customer's physical or mental condition limits their capability to work such that it is not reasonable to require them to work). An ESA customer in the work related activity group must undertake work focused interviews, participate in work related activity and agree an action plan.

"Employment and Support Allowance Work Related Activity Group" means following a Work Capability Assessment DWP will place Customers in either the work-related activity group (WRAG) or support group if they are entitled to ESA. DWP expect Customers in the WRAG to attend regular interviews with an advisor who can help with things like job goals and improving skills.

"**Environmental Information Regulations**" means the Environmental Information (Scotland) Regulations 2004 (and any subordinate regulations made under them from time to time or any superseding or amending regulations) together with any guidance and/or codes or practice issued by the Information Commissioner, the Scottish Information Commissioner and/or any relevant government department in relation to such regulations.

"**ESPD**" means the European Single Procurement Document completed by the Contractor and sent to the Authority on 23rd May 2017.

"**Equipment**" means equipment, computer systems, (including hardware, software and peripherals plant, tackle, materials and other items supplied and used by the Service Provider's Representatives in the performance of the Service Provider's obligations under the Contract.

"**Exit Management**" means the obligations and rights of the Parties to ensure a smooth transition of the Contract from the Service Provider to the Purchaser or any Replacement Service Provider as set out in Clause 59 (Exit Management) and Schedule 10 (Exit Management).

"**Exit Plan**" means the exit plan to be developed and updated by the Service Provider in accordance with Schedule 10 (Exit Management).

"Experience Panel" means the Scottish Government are setting up a series of Experience Panels to gather feedback on the roll-out of devolved Benefits across

Scotland. A specific Experience Panel for Employability Services is being developed. There will be a choice of activities e.g. short surveys, interviews, discussion groups and these may be carried out face-to-face, by phone or online. All materials relating to the Experience Panel recruitment and activity will be provided by The Scottish Government.

"**FOISA**" means the Freedom of Information (Scotland) Act 2002 and any subordinate legislation made under this Act from time to time or any superseding or amending enactments or regulations, together with any guidance and/or codes of practice issued by the Information Commissioner, the Scottish Information Commissioner and/or any relevant government department in relation to such legislation.

"**Force Majeure**" means any event or occurrence which is outside the reasonable control of the Party concerned and which is not attributable to any act or failure to take preventative action by that Party, including industrial action, fire, flood, violent storm, pestilence, explosion, malicious damage, armed conflict, acts of terrorism, nuclear, biological or chemical warfare, or any other disaster, natural or man-made.

"**Good Industry Practice**" means standards, practices, methods and procedures conforming to legal and regulatory requirements and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking as the Service Provider under the same or similar circumstances.

"**Go Live Services**" means the service delivery go live (i.e. Customer start) services to be performed by the Service Provider as outlined in Schedule 1 (Specification and Service Levels).

"Government Gateway" means a secure authentication route into Government IT services.

"Guaranteed Service Standards" means the minimum level of support all Customers accessing the Service must receive regardless of who they are and where they live. The guarantee will include the frequency of meetings and interventions with customers, the development of a tailored action plan and the support they will receive to remain in work when they get a job.

"**Implementation Plan**" means the Initial Implementation Plan until it is superseded by the Detailed Implementation Plan (as subsequently updated in accordance with paragraph 40 (Mobilisation and Implementation) of Schedule 1 (Specification and Service Levels).

"**Incoming Employees**" means individuals whose employment transfers to the Service Provider on the commencement of the provision of the Services by operation of TUPE.

"Individual Placement and Support" or ""**IPS**" means a supported employment model that works with people diagnosed with severe and enduring mental illness to help them find sustainable, competitive jobs in the community that fits their needs and interests. A key principle of IPS is that employment specialists and clinical teams work together to support people to gain employment. Other principles of IPS match the principles of supported employment, as laid out in the Supported Employment Framework for Scotland - for instance, it provides vocational profiling, job finding and employer Engagement as well as person-centred on and off the job support and aftercare. Often the job search part of the process can be much more rapid in IPS than in the traditional supported employment model.

"**Initial Implementation Plan**" means the document entitled Implementation Plan as set out in Schedule 13 (Implementation Plan).

"**Initial Referral Period**" has the meaning set out in clause 4.1.1.

"**Intellectual Property Rights**" means patents, inventions, trade marks, service marks, logos, design rights (whether registerable or otherwise), applications for any of the foregoing, copyright, database rights, domain names, trade or business names, moral rights and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom) and the right to sue for passing off.

"Intermediate Labour Market (ILM)" means a model of waged work in specially created temporary jobs.

"**ITT**" means the Purchaser's invitation to tender dated 9th March 2017.

"**JCP**" or "**Jobcentre Plus**" means Jobcentre Plus being a government-funded employment agency and social security office, whose aim it is to help people of working age find employment in the UK.

"Job Analysis" means once a suitable job is identified for a Customer, a job analysis can be undertaken. This checks any assumptions made in the job description and thoroughly investigates the job on offer so that all elements of the job and the work place are understood. This can include job duties, hours and days of work, health and safety considerations, accessibility, and workplace culture. The job analysis might point towards ways of carving parts of job descriptions that suit the workers' talents, or creating new job descriptions that suit the worker and are cost effective for the employer.

"Jobseekers Allowance" an allowance payable to Customers who are out of work, or working less than 16 hours a week, are aged under pension age and are actively seeking and capable of work.

"**Job Outcome**" means the outcomes as detailed in the first Key Performance Indicator in Annex E to Schedule 1 (Specification and Service Levels).

"**Judicial Order**" means an ineffectiveness order or an order shortening the duration of the contract made in relation to the Contract under Chapter 6 of the Public Contracts (Scotland) Regulations 2015.

"**Key Individuals**" means the Service Provider Representatives identified as being key individuals for the provision of the Services as set out in Schedule 5 (Key Individuals).

"**Key Delivery Indicator**" or "**KDI**" means the key delivery indicators as outlined in Annex F to Schedule 1 (Specification and Service Levels).

"**Key Performance Indicator**" or "**KPI**" means the key performance indicators as outlined in Annex E to Schedule 1 (Specification and Service Levels).

"KPI Failure" means a failure to meet the minimum performance expectations (or any higher standard outlined in Annex 2 of the Pricing Schedule, where relevant) in respect of the KPIs.

"**Law**" means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Service Provider is bound to comply.

"Lot" means the geographical footprint for the specified geographical area in Scotland as set out in Annex C of Schedule 1 (Specification and Service Levels).

"**Management Arrangements**" means the arrangements for the strategic management of the relationship between the Parties, including arrangements for monitoring of the Service Provider's compliance with the Specification, the Service Levels, and the terms of the Contract, set out in Schedule 4 (Management Arranagements).

"**Milestone**" means any event or task which must be completed by a particular date, such as the delivery of a Deliverable, identified as a Milestone in accordance with the the Implementation Plan.

"Milestone Date" means the target date set out against the relevant Milestone in the Implementation Plan by which the Achievement of the Milestone must have been met;

"Milestone Payment" means a payment identified in the Implementation Plan to be made following the Achievement of the relevant Milestone.

"Operational Guidance" means detailed guidance and information (including processes) which is provided by the Scottish Government to the Service Provider to use when delivering the Services.

"**Operational Services**" means any and all of the operational services to be performed by the Service Provider that commence from the first customer referral activity as outlined in Schedule 1 (Specification and Service Levels).

"**Outcomes**" means the Job Outcomes and Sustained Job Outcomes as outlined in Annex E to Schedule 1 (Specification and Service Levels).

"**Outgoing Employees**" means individuals whose employment transfers from the Service Provider on the ceasing of the provision of the Services by the Service Provider by operation of TUPE.

"Parent Company" means any company which is the ultimate Holding Company of the Service Provider and which is either responsible directly or indirectly for the business activities of the Service Provider or which is engaged by the same or similar business to the Service Provider. The term Holding or Parent Company shall have the meaning ascribed by the Companies Act 2006 or any statutory re-enactment or amendment thereto.

"Participation Agreement" means a signed, joint agreement which sets out the commitments of the Service Provider and Customer, and which outlines the service offer and roles and responsibilities for each party.

"Partner Organisation" means the wide range of organisations that support or provide services of potential use to Customers.

"**Party**" means either of the Purchaser or the Service Provider.

"PRaP" means the Provider Referrals and Payments system which enables secure, automated exchanges of information about customers referred to providers, and payments from DWP to Prime Providers. Providers access PRaP securely through the Government Gateway. The PRaP system also provides data about the cost and performance of contracted provision, supporting contract and performance management.

"**Pricing Schedule**" means the details of the pricing of the Services including provision for Service Credits, set out in Schedule 2.

"**Programme**" means the Fair Start Scotland scheme outlined in Schedule 1 (Specification and Service Levels).

"**Purchaser**" means the Scottish Ministers.

"Purchaser Contract Manager" means the individual within the Purchaser's organisation responsible for the day to day management of the Contract.

"**Purchaser Data**" means as defined in Schedule 10 (Exit Management).

"**Purchaser Property**" means any corporeal moveable property issued or made available to the Service Provider by the Purchaser in connection with the Contract.

"**Purchaser Protected Information**" means any information provided by the Purchaser to the Service Provider which:

- carries a protective marking such as "Official", "Secret" or "Top Secret"; or
- is exempt information as set out in Part 2 of FOISA (disregarding for that purpose whether a provision of Part 2 does not confer absolute exemption within the meaning of section 2(2) of FOISA).

"Referral Agency" means any organisation, for example, Jobcentre Plus, Third Sector; Social Service Teams; Carer Groups; Education and Learning institutions, NHS; and Local Authorities that supports a Customer to participate in the Service through a referral to the Service Provider.

"**Referral Period**" means as defined in clause 4.1.1.

"**Relevant Transfer**" has the meaning given in regulation 2(1) of TUPE.

"**Replacement Service Provider**" means any third party service provider appointed to perform the Services by the Purchaser from time to time.

"Retention" means support for employees (or a self-employed people) who become newly disabled, or their existing disability changes in a way that puts their prospects of continued employment at serious risk, to retain current employment. Retention provision via the Programme may extend to Customers who have not been supported by the Service Provider for pre-employment support.

"**Request for Information**" means a request for information within the meaning of section 8 of FOISA or the Environmental Information Regulations and any attempted or apparent such request.

"Scottish Government Performance Management and Operations Support Team" means the team responsible for the day to day contract management of the Contract, their main function is to provide support to the Service Provider and Referral Agencies on administration and performance management of the Programme.

"**Schedule**" means a schedule annexed to, and forming part of, the Contract.

"**Self-employment**" or "**self-employment**" means where the Customer is trading independently for a period of time as defined in the Outcomes.

"**Services**" means any and all of the Services to be supplied by the Service Provider to the Purchaser under the Contract including those set out in the Specification.
"**Service Credits**" means the service credits payable to the Purchaser by the Service Provider in the event that the Service Levels are not met and identified as service credits in the Pricing Schedule.

"**Service Levels**" means the Key Performance Indicators and the Key Delivery Indicators identified as such in the Specification.

"Service Commencement Date" means the date of first Customer Referral activity (i.e. start of operational services 13th March 2018).

"**Services Go-Live Commencement Date**" means the date of the Go Live Customer Service date (3rd April 2018).

"**Service Provider**" means PeoplePlus Group Limited.

"Service Provider Contract Manager" means the individual within the Service Proivder's organisation responsible for the day to day management of the Contract.

"**Service Provider Representatives**" means all persons engaged by the Service Provider in the performance of its obligations under the Contract including:

- its employees and workers (including persons employed by a third party but working for and under the control of the Service Provider);
- its agents, Service Providers and carriers;
- any sub-contractors of the Service Provider (whether approved under clause 34 (Sub-contracting) or otherwise); and
- any other third parties used by the Service Provider in performing the Services or any third parties that the Service Provider refers Customers to as part of the Services.

"**Service Provider Sensitive Information**" means any information provided by the Service Provider to the Purchaser (disregarding any protective marking or assertion of confidentiality) which:

- is specified as Service Provider Sensitive Information in Schedule 7 and has not lost its sensitivity according to the justifications and durations set out in that Schedule; and
- is exempt information pursuant to sections 33(1) or 36, 38 or 39 of FOISA (having regard for that purpose to the public interest there might be in disclosing such information as referred to in section 2(1)(b) of FOISA).

"**Service Provider System**" means the IT components of the system(s) operated by the Service Provider to perform the Services, including all hardware, infrastructure, platforms and software, application platforms and software, database management platforms and data, and third-party software.

"**Service Transfer Date**" means the date on which the Services (or any part of the Services), for whatever reason transfer from the Service Provider to the Purchaser or any Replacement Service Provider.

"**Sites"** means:

(a) any premises (including the Purchaser's premises, the Service Provider's premises or third party premises):

(i) from, to or at which:
(1) the Services are (or are to be) provided; or
(2) the Service Provider manages, organises or otherwise directs the provision or the use of the Services; or

(ii) where: any part of the Service Provider System is situated; or b) any physical interface with the Purchaser's IT system or PRaP takes place.

"SME" means small to medium-sized enterprise which is a business with not more than 250 employees.

"**Specification**" means the Purchaser's general requirements for the provision of services including Service Levels, set out in Schedule 1.

"Stakeholder Engagement Strategy" means a document that details the Service Provider's approach to engaging, collaborating and working effectively and with external stakeholder to enhance Service delivery and maximise Customer outcomes. The strategy must set out how the Service Provider will achieve greater integration with local services and health provision.

"Statutory Referral Organisation" or **"SRO"** means the WFS Statutory Referral Organisation (SRO) responsible for referrals. This must be made by an organisation that has been commissioned by, or has a formal contract or agreement with, an agent of a statutory body; specifically they must act on behalf of a Local Authority or NHS Board, in order to support disabled people with the highest support needs to consider and move into employment, particularly those with learning disabilities and mental health conditions.

"Supported Employment" means an internationally recognised 'place and train' model which enables disabled people to learn on the job with support from colleagues and a job coach. It is based on the principle that disabled people can obtain sustainable work in the open labour market, where they are paid the going rate for the job. In 2010, the Scottish Government published 'A Working Life for All Disabled People' - The Supported Employment Framework for Scotland which sets out our commitment to this model, which is an intensive, personalised asset-based approach.

"Sustained Job Outcome" means the outcomes as detailed in the second and third Key Performance Indicators in Annex E to Schedule 1 (Specification and Service Levels).

"Task Analysis" means looking at specific tasks within the job and developing a logical, step by step process tailored for the individual to help them carry out the task. It can also identify tasks where the individual may require extra support or training. In some cases it can identify where the task should be adapted or where support from colleagues may be necessary.

"**Tender**" means the tender submitted by the Service Provider to the Purchaser in response to the ITT dated 23rd May 2017.

"The Scottish Business Pledge" means that the Scottish Government works with local businesses and authorities to encourage them to implement the Scottish Government Business Pledge, to act on gender balance and inequality and develop city deals to generate business.

"The Scottish Government's Fair Work Agenda" means a shared vision with the Fair Work Convention that by 2025, people in Scotland will have a world-leading working life where fair work drives success, wellbeing and prosperity for individuals, businesses, organisations and society. This vision challenges not only business, employers, unions and the third sector but has clear actions for government.

"The Scottish Living Wage" means the Scottish Living Wage Accreditation Initiative that was established in April 2014 with the aim of increasing the number of employers in Scotland who are recognised for paying their staff the Living Wage. The rate for 2016/17 is £8.45.

"**TUPE**" means the Transfer of Undertakings (Protection of Employment) Regulations 2006.

"Universal Credit: Universal Credit" means a welfare benefit that supports people who are on a low income or out of work due to unemployment or heath issues. It is designed to support households and ensure that where people are working they can sustain that employment and progress towards a life free from benefits.

"Vocational Profiling" means a person-centred tool to assist job seekers make informed choices about job preferences and establish the necessary training and support strategies for on or off the job support.

"Work Capability Assessment" means an assessment that establishes whether an ESA Customer has a limited capability for work and is, therefore, capable of engaging in work-related activity. If they do limited capability they are placed into the ESA Support Group.

"Work Related Activity" means any activity which makes it more likely that a Customer will obtain or remain in work, or be able to do so. Some Customers will be closer to the labour market than others and may be ready to enter work more quickly. Others may need to undertake some more limited activity before moving into paid work.

"**Working Day**" means a day other than a Saturday, Sunday or bank holiday in Scotland, within the meaning of the Banking and Financial Dealings Act 1971.

"**Working Hour**" means an hour between 0900 hours and 1700 hours on a Working Day.

1.2. The interpretation and construction of the Contract is subject to the following provisions:

1.2.1. words importing the singular meaning include, where the context so admits, the plural and vice versa;

1.2.2. words importing the masculine include the feminine and neuter;

1.2.3. reference to a clause is a reference to the whole of that clause unless stated otherwise;

1.2.4. references to any statute, enactment, order, regulation or other similar instrument are construed as a reference to the instrument as amended by any subsequent instrument or re-enacted;

1.2.5. references to any person include natural persons and partnerships, firms and other incorporated bodies and all other legal persons of whatever kind and however constituted and their successors and permitted assignees or transferees;

1.2.6. reference to "expiry or termination" of the Contract includes the making of a Judicial Order;

1.2.7. the words "include", "includes" and "including" are to be construed as if they were immediately followed by the words "without limitation"; and

1.2.8. headings are included in the Contract for ease of reference only and do not affect the interpretation or construction of the Contract.

2. Condition Precedent: Requirement for a Parent Company Guarantee

It shall be a condition of this Contract that, if required by the Purchaser, the Service Provider shall deliver a validly executed parent company guarantee in the form set out in Schedule 8 (Parent Company Guarantee). The rights and obligations of the Parties shall have no force or effect unless the parent company guarantee has been properly executed and delivered to the Purchaser. The parties acknowledge that if this condition has not been fulfilled any performance of this Contract by the Service Provider shall be at the risk of the Service Provider and the Purchaser shall not be liable for and the Service Provider irrevocably waives any entitlement to payment of any fees, expenses or other payments in relation to such performance. Where the Service Provider has failed to fulfil this condition within 14 days of the Effective Date the Purchaser shall have the right to terminate the Contract by notice in writing to the Service Provider.

3. Nature of the Contract

3.1. The Contract is a public services contract within the meaning of regulation 2(1) of the Public Contracts (Scotland) Regulations 2015.

3.2. The Service Provider acknowledges that it is not the exclusive Service Provider of the Services to the Purchaser and as such no guarantee of work or volume of work has been granted or given by the Purchaser.

4. Period

4.1. Subject to the remainder of this clause 4 the period of the Contract is from and including the Effective Date to and including 2 April 2021 (unless it is terminated earlier in accordance with the provisions of the Contract), provided always that:-

4.1.1. the Service Provider shall only be entitled to receive Customer referrals pursuant to the Contract during the period commencing on the Service Commencement Date and ending on 2 April 2021 (the "**Initial Referral Period**"); and

4.1.2. the Contract shall continue for the period from (and including) 3 April 2021 in respect of those referrals made to the Service Provider prior to the expiry of the Initial Referral Period in so far as required as part of the Services which potentially could be to and including 24th November 2023.

(the "**Contract Period**").

4.2. The Purchaser may at its sole option extend the Initial Referral Period in accordance with the following provisions:

4.2.1. the Purchaser may extend the Initial Referral Period for an additional period up to (and including) 3 April 2022 by providing the Service Provider with at least sixty (60) Working Days' notice prior to the expiry of the Initial Referral Period ("**Extended Referral Period One**"); and

4.2.2. the Purchaser may extend Extended Referral Period One for an additional period up to (and including) 4 April 2023 by providing the Service Provider with at least sixty (60) Working Days' notice prior to the expiry of Extended Referral Period One ("**Extended Referral Period Two**").

4.3. Where the Initial Referral Period is extended in accordance with clause 4.2.1, clause 4.1.2 shall not apply and the Contract shall continue in respect of those referrals made to the Service Provider prior to the expiry of Extended Referral Period One in so far as required as part of the Services which potentially could be to and including 24th November 2024.

4.4. Where the Extended Referral Period One is extended in accordance with clause 4.2.2, clause 4.3 shall cease to apply and the Contract shall continue in respect of those referrals made to the Service Provider prior to the expiry of Extended Referral Period Two in so far as required as part of the Services which potentially could be to and including 24th November 2025.

4.5. Any further contractual terms required to give effect to the extensions outlined in this clause 4 shall continue in so far as necessary to take account of the relevant extension (.e.g. invoicing provisions).

5. Break

The Purchaser may terminate the Contract at any time by giving not less than three (3) months' notice to the Service Provider.

5.A Implementation

5A.1 The Service Provider shall:

5A.1.1 comply with the Implementation Plan; and

5A.1.2 ensure that each Milestone is Achieved on or before its Milestone Date.

5A.2 The Service Provider shall prepare and deliver the Detailed Implementation Plan to the Purchaser in accordance with Schedule 1 (Specification and Service Levels).

5A.3 If, at any time, the Service Provider becomes aware that it will not (or is unlikely to) successfully achieve any Milestone by the applicable Milestone Date, it shall immediately notify the Purchaser of the fact of the Delay, the reasons for the Delay, the consequences of the Delay for the rest of the Implementation Plan and how the Service Provider proposes to mitigate the Delay.

5A.4 Whether the Delay is due to the Purchaser's Default or not, the Service Provider shall deploy all additional resources and efforts, and take all reasonable steps, to eliminate or mitigate the consequences of the Delay.

5A.5 Where the Service Provider incurs additional costs as a result of any action taken or required to be taken in accordance with clause 5A.4 the Service Provider shall not be entitled to recover these from the Authority.

6. Specification and Service Levels

The Service Provider must comply with the Specification. In particular, the Service Provider must meet or exceed the Service Levels.

7. **Pricing Schedule**

7.1 The Pricing Schedule sets out details of the pricing of the Services including provision for Service Credits.

7.2. Accordingly, the Service Provider may not unilaterally increase the prices in the Pricing Schedule. For the avoidance of doubt nothing in the Contract shall prevent the Service Provider from reducing the Contract Charges.

8. Management Arrangements

8.1. The Service Provider must maintain the capacity to supply the Services throughout the Contract Period.

8.2. The Parties must comply with the Management Arrangements.

SECTION B: MISCELLANEOUS PROVISIONS INCLUDING THOSE RELATING TO PRICE, PAYMENT AND INFORMATION

9. Service Provider's Status

At all times during the Contract Period the Service Provider is an independent service provider and nothing in the Contract establishes a contract of employment, a relationship of agency or partnership or a joint venture between the Parties or between the Purchaser and any Service Provider Representative. Accordingly, neither Party is authorised to act in the name of, or on behalf of, or otherwise bind the other Party save as expressly permitted by the terms of the Contract.

10. Notices

10.1. Any notice or other communication which is to be given by a Party to the other under the Contract must be:

10.1.1. given in writing;

10.1.2. addressed in accordance with clause 10.3; and

10.1.3. sent by letter (delivered by hand, first class post or by recorded delivery or special delivery), fax or e-mail.

10.2. Provided the relevant communication is not returned or rejected as undelivered, the notice or communication is deemed to have been given:

10.2.1. 2 Working Days after the day on which the letter was posted; or

10.2.2. 4 Working Hours after the communication was sent, in the case of fax or email.

10.3. For the purposes of this clause, the address of each Party is:

10.3.1. For the Purchaser:
Scottish Government, More Powers Implementation Team, Victoria Quay, Edinburgh, EH6 6QQ
For the attention of [redacted]
Tel: [redacted]
[redacted]@gov.scot

10.3.2. For the Service Provider:
PeoplePlus Group Limited, Blades Enterprise Centre, John Street, Sheffield S2 4SW
For the attention of: [redacted]
Tel: [redacted]
E-mail: [redacted]@peopleplus.co.uk

10.4. Either Party may change its address details by serving a notice in accordance with this clause.

10.5. Notices under clause 58.1 (Termination on Insolvency or Change of Control) may be sent to the Purchaser's trustee, receiver, liquidator or administrator, as appropriate.

11. Price

11.1. In consideration of, but subject always to, the Service Provider's performance of the Services in accordance with the Contract, the Purchaser will pay:

11.1.1. the price due in accordance with the Pricing Schedule; and

11.1.2. a sum equal to the value added tax chargeable at the prevailing rate.

11.2. The Service Provider may not suspend the provision of the Services if it considers that the Purchaser has failed to pay the price due.

12. Payment and Invoicing

12.1. The Purchaser must pay all sums due to the Service Provider within 30 days of receipt of a valid invoice.

12.2. The Service Provider must render invoices monthly in arrears.

12.3. The Service Provider must ensure that each invoice contains the appropriate Contract references details of any Service Credits applied and a detailed breakdown of the Services provided. The Service Provider must supply such other documentation reasonably required by the Purchaser to substantiate any invoice.

12.4. Value added tax, where applicable, must be shown separately on all invoices as a strictly net extra charge.

12.5. Where any Service Credits are due to the Purchaser these shall be credited against the next invoice rendered by the Service Provider. Where no invoice is due or likely to be rendered for a period exceeding 2 months from the date the relevant Service Credit is incurred, the Service Provider must promptly issue a credit note to the Purchaser and pay the credited sum to the Purchaser within 30 days of issue.

12.6. Interest is payable on the late payment of any undisputed sums of money in accordance with the Late Payment of Commercial Debts (Interest) Act 1998. In the case of sums due by the Purchaser, the sums referred to in this clause must be properly invoiced by the Service Provider.

12.7. The Service Provider shall indemnify the Purchaser on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Purchaser at any time in respect of the Service Provider's failure to account for or to pay any VAT relating to payments made to the Service Provider under this Contract. Any amounts due under this clause 12.7 shall be paid in cleared funds by the Service Provider to the Purchaser not less than five Working Days before the date upon which the tax or other liability is payable by the Purchaser.

12.8 The Service Provider shall only be entitled to claim for payments in respect of Outcomes as outlined in the Pricing Schedule for the period of three (3) months after the expiry of the Contract Period.

13. Recovery of Sums Due

13.1. Wherever under the Contract any sum of money is recoverable from or payable by the Service Provider to the Purchaser, the Purchaser may deduct that sum from any sum due to the Service Provider whether under the Contract or otherwise.

13.2. The Service Provider must make any payments due to the Purchaser without any deduction whether by way of set-off, counterclaim, discount, abatement or otherwise unless the Service Provider has a valid court order requiring an amount equal to such deduction to be paid by the Purchaser to the Service Provider.

14. Data Protection Act

14.1. For the purposes of this clause, the terms “Data Controller”, “Data Processor”, “Data Subject”, “Personal Data” and “Processing” have the meanings given in section 1(1) of the Data Protection Act 1998.

14.2. The Service Provider shall:

14.2.1. at all times comply with the Data Protection Act 1998 (including any subordinate legislation made thereunder and any guidance and/or codes of practice issued by the Information Commissioner from time to time in relation thereto) and shall not perform its obligations in such a way so as to cause the Purchaser to breach any of its obligations under the Data Protection Act 1998;

14.2.2. comply with the terms of any Data Sharing Protocol; and

14.2.3. provide all assistance, support and information required by the Purchaser in order for the Purchaser to comply with any of its obligations under the Data Protection Act 1998.

14.3. Where the Service Provider Processes Personal Data as a Data Processor for the Purchaser the Service Provider must:

14.3.1. enter into a data processing agreement in the form set out in Schedule 9 annexed hereto, and only process the Personal Data in accordance with any instructions as may be given by the Purchaser (which may be specific or of a general nature);

14.3.2. process the Personal Data only to the extent, and in such manner as is necessary for the performance of the Service Provider’s obligations under the Contract or as is required by the Law;

14.3.3. implement appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, such measures being appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;

14.3.4. obtain approval before transferring the Personal Data to any sub-contractor engaged by the Service Provider in connection with the provision of the Services (or any part of them);

14.3.5. not transfer or cause or permit the Personal Data to be transferred outside of the European Economic Area without Approval and, where the Purchaser does approve the transfer, to comply with the obligations of a Data Controller under the Eighth Data Protection Principle (as set out in Schedule 1 to the Data Protection Act 1998) and any instructions notified to the Service Provider by the Purchaser;

14.3.6. provide a written description of the technical and organisational measures employed by the Service Provider for Processing Personal Data and permit the Purchaser (on reasonable notice) to inspect and audit the Service Provider's Processing activities;

14.3.7. ensure that all Service Provider Representatives accessing the Personal Data are competent and trained in the law of data protection and that such Service Provider Representatives are aware of the confidential nature of the Personal Data and comply with the obligations set out in this clause;

14.3.8. not disclose or divulge (and ensure that the Service Provider Representatives do not disclose or divulge) any of the Personal Data to any third parties unless directed in writing to do so by the Purchaser;

14.3.9. allow for and contribute to audits to demonstrate compliance with this clause 14, including inspections, conducted by the Purchaser or another auditor mandated by the Purchaser;

14.3.10. inform the Purchaser immediately if, in the opinion of the Service Provider, an instruction given pursuant to clause 14.3.9 infringes any Law;

14.3.11. inform the Purchaser immediately if it becomes aware of any Personal Data breach providing such information in relation to the breach and the circumstances as the Purchaser may require and the Service Provider shall take such steps (at its cost) as the Purchaser may require in order to remedy or mitigate the breach;

14.3.12. comply with any instructions from the Purchaser in terms of the deletion or return of any Personal Data at the end of the Contract Period including those outlined in the Exit Plan; and

14.3.13. include in any sub-contracts with sub-contractor approved in accordance with clause 14.3.4 equivalent provisions as least as onerous as those set out in this clause 14.

14.3 The Service Provider must notify the Purchaser promptly, and in any event within 5 Working Days, if it receives:

14.3.1. a request from a Data Subject to have access to their Personal Data;

14.3.2 a complaint or request relating to the Purchaser's obligations under the Data Protection Act 1998;

and the Service Provider shall provide the Purchaser with full cooperation and assistance in relation to any complaint or request made.

14.4 Where the Service Provider is collecting Personal Data, the Service Provider must comply with all the fair processing provisions under the Data Protection Act 1998, and must notify the Data Subjects that the Personal Data collected by the Service Provider may be shared with the Purchaser.

14.5 The Service Provider shall indemnify the Purchaser and hold it harmless from and against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Purchaser may suffer or incur as a result of or in connection with any breach of this clause 14.

14.6 To comply with section 31(3) of the Public Services Reform (Scotland) Act 2010, the Purchaser publishes an annual statement of all payments over £25,000. In addition, in line with openness and transparency, the Scottish Government publishes a monthly report of all payments over £25,000. The Service Provider should note that where a payment is made in excess of £25,000 there will be disclosure (in the form of the name of the payee, the date of the payment, the subject matter and the amount of payment) in the both the monthly report and the annual Public Services Reform (Scotland) Act 2010 statement.

15. Freedom of Information

15.1 The Service Provider acknowledges that the Purchaser is subject to the requirements of FOISA and the Environmental Information Regulations and undertakes to assist and cooperate with the Purchaser to enable the Purchaser to comply with FOISA and the Environmental Information Regulations.

15.2 If the Service Provider receives a Request for Information the Service Provider must promptly respond to the applicant. Where the Request for Information appears to be directed to information held by the Purchaser, the Service Provider must promptly inform the applicant in writing that the Request for Information can be directed to the Purchaser.

15.3 Where the Purchaser receives a Request for Information concerning the Contract, the Purchaser is responsible for determining at its absolute discretion whether information requested is to be disclosed to the applicant or whether the information requested is exempt from disclosure in accordance with FOISA or the Environmental Information Regulations.

15.4 The Service Provider acknowledges that the Purchaser may, acting in accordance with the Purchaser's Code of Practice on the Discharge of Functions of Public Authorities issued under section 60 of FOISA (as may be issued and revised from time to time), be obliged under FOISA or the Environmental Information Regulations to disclose information requested concerning the Service Provider or the Contract:

15.4.1 in certain circumstances without consulting the Service Provider, or

15.4.2 following consultation with the Service Provider and having taken its views into account.

15.5 Where clause 15.4 applies the Purchaser must take reasonable steps, where practicable, to give the Service Provider advance notice of the fact of disclosure or, failing that, draw the fact of disclosure to the attention of the Service Provider after such disclosure.

15.6 Where a Request for Information concerns Service Provider Sensitive Information specified in Schedule 7 (Service Provider Sensitive Information) (having regard to the justifications and durations set out there), the Purchaser must take reasonable steps, where practicable, to consult with the Service Provider before disclosing it pursuant to a Request for Information.

16 Purchaser Protected Information

16.1 The Service Provider must:

16.1.1 treat all Purchaser Protected Information as confidential and safeguard it accordingly, implementing appropriate technical and organisational measures to protect Purchaser Protected Information against disclosure;

16.1.2 only use the Purchaser Protected Information for the purposes of performing its obligations under the Contract;

16.1.3 only disclose the Purchaser Protected Information to such Service Provider Representatives that are directly involved in the performance of the Contract and need to know the information for such performance; and

16.1.4 not disclose any Purchaser Protected Information without the prior written consent of the Purchaser.

16.2 The Service Provider must immediately notify the Purchaser of any breach of security concerning the Purchaser Protected Information, providing such information in relation to the breach and the circumstances as the Purchaser may require. The Service Provider must take

such steps (at its cost) as the Purchaser may require in order to remedy or mitigate the breach and fully co-operate with the Purchaser in any investigation that the Purchaser considers necessary to undertake as a result of any such breach of security.

16.3 Clause 16.1 does not apply to the extent that:

16.3.1 disclosure is required by law or by order of any competent court or tribunal;

16.3.2 information is in the possession of the Service Provider without restriction as to its disclosure prior to its disclosure by the Purchaser;

16.3.3 information is obtained from a third party (who lawfully acquired it) without restriction as to its disclosure;

16.3.4 information is already in the public domain at the time of disclosure otherwise than by a breach of the Contract; or

16.3.5 information is independently developed without access to the Purchaser Protected Information.

16.4 Breach of this clause or the Official Secrets Acts 1911 to 1989 by the Service Provider is a material breach for the purposes of clause 57.1.3 (Termination Rights).

17 Service Provider Sensitive Information

17.1 The Purchaser must:

17.1.1 treat all Service Provider Sensitive Information as confidential and safeguard it accordingly; and

17.1.2 not disclose any Service Provider Sensitive Information to any other person without the prior written consent of the Service Provider.

17.2 Clause 17.1 does not apply to the extent that:

17.2.1 disclosure is required by law or by order of any competent court or tribunal;

17.2.2 information is in the possession of the Purchaser without restriction as to its disclosure prior to its disclosure by the Service Provider;

17.2.3 information is obtained from a third party (who lawfully acquired it) without restriction as to its disclosure;

17.2.4 information is already in the public domain at the time of disclosure otherwise than by a breach of the Contract; or

17.2.5 information is independently developed without access to the Service Provider Sensitive Information.

17.3 Nothing in this Contract prevents the Purchaser from disclosing any Service Provider Sensitive Information or any other information concerning the Service Provider or the Contract:

17.3.1 pursuant to a Request for Information concerning the information (see clause 15 (Freedom of Information);

17.3.2 in accordance with the Purchaser's publication scheme (within the meaning of section 23 of FOISA) as reviewed from time to time;

17.3.3 in accordance with the requirements of Part 3 of the Public Services Reform (Scotland) Act 2010;

17.3.4 in accordance with any future policies of the Purchaser concerning the routine disclosure of government information in the interests of transparency;

17.3.5 to any consultant, Service Provider or other person engaged by the Purchaser, for example to conduct a gateway review;

17.3.6 in response to a Parliamentary Question from a Member of the Scottish Parliament, a member of the United Kingdom Parliament, or any other department, office or agency of Her Majesty's Government in Scotland or the United Kingdom, and their servants or agents, and when disclosing such information to either the Scottish Parliament or the United Kingdom Parliament it is recognised and agreed by both parties that the Purchaser shall if the Purchaser sees fit disclose such information but is unable to impose any restrictions upon the information that the Purchaser provides to Members of the Scottish Parliament or Members of the United Kingdom Parliament;

17.3.7 in response to any inquiry of the European Commission concerning the Contract; or

17.3.8 for the purpose of any examination by any auditors of the Purchaser (including Audit Scotland, the Auditor General for Scotland and the Scottish Parliament) of the economy, efficiency and effectiveness with which the Purchaser has used its resources.

17.4 The Service Provider consents to the publication of the Contract by the Purchaser, subject to such redactions as the Purchaser may decide to make. The Purchaser may consult with the Service Provider to inform its decisions concerning redaction (for example to exclude any Service Provider Sensitive Information) but any decisions taken by the Purchaser are final and conclusive.

18 Audit and Records Management

18.1 In this Clause 18, the following terms have the following meanings:-

The '**Act**' means the Public Records (Scotland) Act 2011; and

'**Records Management Plan'** means the plan prepared by the Purchaser and approved by the Keeper of the Records of Scotland under section 1 of the Act.

18.2 The Service Provider must retain and maintain until 5 years after the end of the Contract Period full and accurate records of the Contract including the Services provided and payments made and reimbursed under it.

18.3 The Service Provider must on request, and without any charge to the Purchaser, afford the Purchaser, or the Purchaser's representatives, such access to those records as may reasonably be requested by the Purchaser in connection with the Contract.

18.4 The Service Provider shall, for the duration of the Contract, provide the Purchaser with all assistance requested by the Purchaser acting reasonably to assist the Purchaser in complying with its obligations under the Act and with the Purchaser's Records Management Plan where such compliance is in respect of records created or to be created by the Service Provider on behalf of the Purchaser in terms of this Contract. This assistance will be at no cost to the Purchaser.

18.5 At the end of the Contract Period, the Service Provider shall transfer the records in question to the Purchaser, such transfer to include full ownership of the records including all Intellectual Property Rights in relation thereto. The transfer shall be at no cost to the Purchaser. The

Service Provider shall ensure that all relevant information reasonably required to locate individual items within the records, including metadata and database schema, are also offered to the Purchaser on the same terms.

18.6 If the Service Provider shall become bankrupt (whether voluntarily or compulsorily), unable to pay its debts, insolvent or make arrangements with its creditors or if any resolution is adopted for the winding up of any party, or if a receiver, administrator or administrative receiver is appointed over the whole or any part of its assets or if either party goes into liquidation (whether voluntarily or compulsorily), otherwise than for the purposes of amalgamation or reconstruction or any form of execution levied upon its assets, then immediately upon the occurrence of any of these events, the records which would, in terms of clause 18.5 fall to be offered to the Purchaser shall be deemed to be held on trust by the Service Provider on behalf of the Purchaser as the Purchaser's agent. The Service Provider shall thereafter, if and when so required by the Purchaser, transfer the records in question to the Purchaser, such transfer to be on the same terms as would apply to a transfer made in terms of clause 18.5.

19 Publicity

The Service Provider must not make any press announcement or otherwise publicise the Contract in any way, except with the written consent of the Purchaser.

SECTION C: PROVISION OF SERVICES

20 Provision of the Services

20.1 The Service Provider must provide the Services:

20.1.1 in accordance with the Specification the Service Levels;

20.1.2 to the satisfaction of the Purchaser acting reasonably.

20.2 The Service Provider acknowledges that the Purchaser relies on the skill, care, diligence and judgment of the Service Provider in the supply of the Services and the performance of its obligations under the Contract.

20.3 The Service Provider must at all times implement, maintain and comply with the BCDR Plan.

21 Deliverables and Milestones

21.1 The Service Provider must provide the Services, including any Deliverables:

21.1.1 at the date(s), time(s) and location(s) required by the Purchaser; and

21.1.2 in good time to meet any Milestones required by the Purchaser.

21.2 When the Service Provider believes acting reasonably that it has provided any Deliverable or completed any Milestone in accordance with the Contract it must notify the Purchaser.

21.3 The Purchaser may thereafter by notice to the Service Provider:

21.3.1 accept the provision of the Deliverable or the completion of the Milestone (as appropriate), having regard to the Achievement criteria or any other acceptance criteria set out in the Implementation Plan or otherwise communicated to the Service Provider in writing; or

21.3.2 providing reasons, reject the provision of the Deliverable or the completion of the Milestone.

21.4 Where the Purchaser rejects the completion of a Milestone or provision of a Service or Deliverable in accordance with clause 21.3.2, the Service Provider must at its expense immediately rectify or remedy any defects and/or delays.

21.5 Risk and ownership in any Deliverables that are corporeal moveables and in any physical media in which any Deliverables are delivered vests in the Purchaser upon acceptance in accordance with this clause.

21.6 Whether the defect or delay is due to the Purchaser or not, the Service Provider shall deploy all additional resources to address the consequences of the default or delay. Where such default or delay is solely due to the Purchaser, any additional costs in respect of the said additional resources shall be agreed between the parties both acting reasonably.

21A. Assurance and Fraud Reviews

21A.1. The Service Provider must comply with the Purchaser's requirements as notified to the Service Provider by the Purchaser from time to time in respect of the three key Service Provider Assurance Areas described in clause 21A.2 below (the "**Provider Assurance Requirements**").

21A.2. The Purchaser will periodically throughout the Contract Period carry out review(s) (the "**Assurance and Fraud Review(s)**") of the Service Provider in three key Service Provider Assurance Areas:

a) **Governance Arrangements** – to ensure the Service Provider's has robust governance arrangements, systems for tracking and reporting performance and anti-fraud measures;

b) **Service Delivery** – to ensure the Service Provider's has effective systems for administering the Customer journey to ensure that the Purchaser is receiving the service it is paying for. The review will also include the management of the supply chain;

c) **Financial Procedures** – to ensure the Service Provider has effective systems in place to support their claims for payment, including appropriate segregation of duties.

21A.3. On completion of each Assurance and Fraud Review by the Purchaser, the Service provider will be awarded a Service Provider Assurance and Fraud Rating: (i) weak; or (ii) limited; or (iii) reasonable; or (iv) strong (the "**Assurance and Fraud Rating**").

21A.4. The frequency and manner of carrying out the Assurance and Fraud Reviews shall be determined at the absolute discretion of the Purchaser.

21A.5. The Purchaser shall send a formal report (the "**Assurance and Fraud Review Report**") to the Service Provider which will set out (i) the Assurance and Fraud Rating; (ii) key strengths; and (iii) weaknesses/areas for improvement.

21A.6. Without prejudice to clause 21A.9, where weakness/areas for improvement have been set out in the Assurance and Fraud Review Report, the Service Provider must submit to the Purchaser for its approval an action plan (the "**Service Provider Assurance Action Plan**") setting out appropriate steps and a proposed timetable for how the Service Provider proposes to remedy such weaknesses/areas for improvement. The Service Provider must submit the Service Provider Assurance Action Plan to the Purchaser within ten (10) Working Days (or such other period of time as notified by the Purchaser) of receipt of the Assurance and Fraud Review Report. Once the Service Provider Assurance Action Plan has been approved by the Purchaser, the Service Provider must implement it in accordance with the timetable set out in the Service Provider Assurance Action Plan.

21A.7. Where the Purchaser rejects the Service Provider Assurance Action Plan, the Service Provider shall address all of the Purchaser's concerns in a revised Service Provider Assurance Action Plan, which it shall submit to the Purchaser within a period of ten (10) Working Days (or such other period as notified by the Purchaser) of its receipt of the Purchaser's comments.

21A.8. In the event of failure to agree a timescale for the completion of the Service Provider Assurance Action Plan then the Service Provider shall have no longer than twenty eight (28) Working Days from the date of receipt to remedy the action points identified in the Service Provider Assurance and Fraud Review Report.

21A.9. Where a Service Provider Assurance Action Plan, submitted by the Service Provider is approved by the Purchaser, such approval shall not relieve the Service Provider of its obligations to remedy and weaknesses/areas for improvement set out in the Service Provider Assurance and Fraud Review Report and ensure that it does not receive a "Weak" or "Limited" Assurance and Fraud Rating in any further Service Provider Assurance and Fraud Review.

21A.10. The Purchaser accepts no liability whatsoever in respect of the content, suitability or implementation of a Service Provider Assurance Action Plan. Any assistance or advice the Purchaser may offer, or any act or omission of the Purchaser, in connection with a Service Provider Assurance Action Plan shall not relieve the Service Provider of its obligations to remedy any weaknesses/areas for improvement set out in the Service Provider Assurance and Fraud Review Report and ensure that it does not receive a "Weak" or "Limited" Assurance and Fraud Rating in any further Service Provider Assurance and Fraud Review.

21A.11. Notwithstanding that the Service Provider may have submitted and the Purchaser may have approved a Service Provider Assurance Action Plan, where a Service Provider is awarded a "Weak" or "Limited" Assurance and Fraud Rating it shall remain the Service Provider's responsibility, at its own expense, to deploy, all resources and take all action(s) necessary to remedy the "Weak" or "Limited" Assurance and Fraud Rating and ensure that it does not receive a "Weak" or "Limited" Assurance and Fraud Rating in any further Service Provider Assurance and Fraud Review.

21A.12. Failure by the Service Provider, at its own expense to deploy all resources and take all action(s) necessary to remedy the "Weak" or "Limited" Assurance and Fraud Rating shall constitute a Default by the Service Provider.

21A.13. Failure by the Service Provider:

i. to submit a Service Provider Assurance Action Plan; and/or:

ii. to submit a Service Provider Assurance Action Plan within ten (10) Working Days (or such other time period as agreed in writing by the Purchaser) of receipt of the Service Provider Assurance and Fraud Review Report; and/or

iii. to implement a Service Provider Assurance Action Plan, which has been approved by the Purchaser, in a accordance with the timetable set out in the Service Provider Assurance Action Plan;

shall constitute a Default by the Service Provider.

21A.14. The Purchaser is entitled to regard the following circumstances, without limitation, to be a material breach of the Contract which shall entitle it to terminate in accordance with clause 57.1.3 (Termination Rights).

a) Where the Service Provider has been awarded an Assurance and Fraud Rating of "Weak" or "Limited", as notified to the Service Provider by the Purchaser from time to

time, in two (2) separate consecutive Service Provider Assurance and Fraud Reviews for reasons which the Purchaser regards, at its sole discretion, as similar reasons; or

b) Where the Service Provider has been awarded an Assurance and Fraud Rating of "Weak" or "Limited" as notified to the Service Provider by the Purchaser from time to time, in three (3) separate consecutive Service Provider Assurance and Fraud Reviews regardless of the reasons for such award.

21A.15. Notwithstanding any other term of the Contract, the Service Provider hereby gives its consent for the Purchaser to publish from time to time any of the Service Provider's Assurance and Fraud Ratings to the general public and to provide the Service Provider's Assurance and Fraud Ratings to any person as the Purchaser deems appropriate. The Service Provider shall assist and cooperate with the Purchaser to enable the Purchaser to publish and provide the Service Provider's Assurance and Fraud Ratings to any person the Purchaser deems appropriate in accordance with this clause.

SECTION D: STAFF INVOLVED IN THE PROVISION OF SERVICES

22 Key Individuals

22.1 The Service Provider acknowledges that the Key Individuals are essential to the proper provision of the Services to the Purchaser.

22.2 The Key Individuals must not be released from providing the Services without the approval of the Purchaser, except by reason of long-term sickness, maternity, paternity, adoption or parental leave, termination of employment or equivalent extenuating circumstances. Where such extenuating circumstances arise or are foreseeable, the Service Provider must immediately give notice of that fact to the Purchaser.

22.3 The Service Provider may propose a replacement to a Key Individual (and must do so when a Key Individual is to be released from providing the Services), in which case:

22.3.1 appropriate arrangements must be made to minimise any adverse impact on the Contract which could be caused by the change in Key Individuals (including, wherever possible, a transfer period of sufficient duration to allow for the transfer of know-how and skills); and

22.3.2 the replacement must be of at least equal status and of equivalent qualifications, experience, training and skills to the Key Individual being replaced and must be fully competent to carry out the responsibilities of that person in relation to the Services.

22.4 Any proposed replacement to a Key Individual is subject to the approval of the Purchaser. Subject to the Service Provider's compliance with this clause, the Purchaser must not unreasonably withhold such approval.

23 Offers of Employment

23.1 For the duration of the Contract and for a period of 12 months thereafter the Service Provider must not employ or offer employment to any of the Purchaser's employees who have been associated with the Contract and/or the contract management of the Contract without the Purchaser's prior approval.

23.2 This clause does not prevent the Service Provider from employing or offering employment to any person who has applied for employment in response to an advertisement placed in the normal course of business and not placed with the objective of soliciting the Purchaser's employees.

24 Staff transfer at commencement

24.1 NOT USED.

24.2 The Parties agree that the commencement of the provision of the Services by the Service Provider may constitute a Relevant Transfer in respect of the Incoming Employees.

24.3 The Service Provider is responsible for all emoluments and outgoings in respect of the Incoming Employees (including, without limitation, all wages, bonuses, commission, premiums, subscriptions, pay as you earn and national insurance contributions and pension contributions) which are attributable in whole or in part to the period from the date of the Relevant Transfer, including bonuses or commission which are payable on or before the date of the Relevant Transfer but attributable in whole or in part to the period from the date of the Relevant Transfer.

24.4 The Service Provider indemnifies the transferor against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and any other liabilities which the transferor may incur in respect of the emoluments and outgoings referred to in clause 24.3.

25 Information about Service Provider Employees

25.1 The Purchaser may by notice require the Service Provider to disclose such information as the Purchaser may require relating to those of the Service Provider's employees carrying out activities under or connected with the Contract.

25.2 The Service Provider must disclose by notice all such information as is required by the Purchaser under clause 25.1, within such reasonable period specified by the Purchaser. The Service Provider acknowledges that the Data Protection Act 1998 does not prevent the disclosure of anonymised data that is not personal data within the meaning of that Act.

25.3 The Service Provider consents to the disclosure by the Purchaser of all information provided by the Service Provider under this clause to other service providers that the Purchaser may invite to tender or appoint for services to be provided in substitution for the Services.

26 Staff transfer on expiry or termination

26.1 NOT USED.

26.2 The Parties agree that the ceasing of the provision of the Services by the Service Provider may constitute a Relevant Transfer in respect of the Outgoing Employees.

26.3 The Service Provider indemnifies the Purchaser and any replacement service provider against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Purchaser or any replacement service provider may suffer as a result of or in connection with:

26.3.1 the provision of information pursuant to clause 25;

26.3.2 any claim or demand by any Outgoing Employee (whether in contract, delict, under statute or otherwise) arising directly or indirectly from any act, fault or omission of the Service Provider in respect of any Outgoing Employee on or before the date of the Relevant Transfer;

26.3.3 any failure by the Service Provider to comply with its obligations under regulations 13 or 14 of TUPE or any award of compensation under regulation 15 of TUPE save where such failure arises from the failure of the Purchaser or any replacement service provider to comply with its obligations under regulation 13 of TUPE; and

26.3.4 any claim (including any individual employee entitlement under or consequent on such a claim) by any trade union or other body or person representing any Outgoing Employees arising from or connected with any failure by the Purchaser to comply with any legal obligation to such trade union, body or person.

26.4 The Service Provider is responsible for all emoluments and outgoings in respect of the Outgoing Employees (including, without limitation, all wages, bonuses, commission, premiums, subscriptions, pay as you earn and national insurance contributions and pension contributions) which are attributable in whole or in part to the period up to and including the date of the Relevant Transfer (including bonuses or commission which are payable after the date of the Relevant Transfer but attributable in whole or in part to the period on or before the date of the Relevant Transfer).

26.5 The Service Provider indemnifies the Purchaser and any replacement service provider against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and any other liabilities which the Purchaser or replacement service provider may incur in respect of the emoluments and outgoings referred to in clause 26.4.

27 Security

27.1 The Service Provider must comply with the Purchaser's policies concerning Baseline Personnel Security Standard clearance and such modifications to those policies or replacement policies as are notified to the Service Provider from time to time.

27.2 The Service Provider must notify the Purchaser of any matter or other change in circumstances which might adversely affect future Baseline Personnel Security Standard clearance.

27.3 The Service Provider must comply with Schedule 12 (Security) at all times when providing the Services.

SECTION E: PROVISIONS RELATING TO INTELLECTUAL PROPERTY AND GOVERNANCE

28 Parties' pre-existing Intellectual Property Rights

Except as expressly provided for in the Contract, neither Party acquires any interest in or license to use the other Party's Intellectual Property Rights as they subsist at the Effective Date or as developed independently of the Contract.

29 Specially Created Intellectual Property Rights

29.1 All Intellectual Property Rights in Deliverables and any reports, guidance, specification, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material prepared by or for the Service Provider in the course of or in connection with the Services for use, or intended use, in relation to the performance by the Service Provider of its obligations under the Contract belong to the Purchaser.

29.2 The Service Provider assigns to the Purchaser, with full title guarantee, all Intellectual Property Rights which may subsist in the materials referred to in clause 29.1. This assignation takes effect on the Effective Date or as an assignation of future rights that will take effect immediately on the coming into existence of the Intellectual Property Rights produced by the Service Provider. The Service Provider must execute all documentation necessary to effect this assignation.

30 Licences of Intellectual Property Rights

30.1 The Service Provider grants to the Purchaser a royalty-free, irrevocable and non-exclusive licence (with a right to sub-licence) to use any Intellectual Property Rights owned or developed prior to the Effective Date and which the Purchaser reasonably requires in order to enjoy the benefit of the Services.

30.2 Not Used

30.3 The Service Provider must ensure that the third party owner of any Intellectual Property Rights that are or which may be used to perform the Contract grants to the Purchaser a royalty-free, irrevocable and non-exclusive licence or, if itself a licensee of those rights, grants to the Purchaser an authorised and equivalently wide sub-licence, to use, reproduce, modify, develop and maintain the Intellectual Property Rights. Such licence or sub-licence must be non-exclusive, perpetual, royalty free and irrevocable.

31 Claims relating to Intellectual Property Rights

31.1 The Service Provider must not infringe any Intellectual Property Rights of any third party in providing the Services or otherwise performing its obligations under the Contract and must ensure that the provision of the Services and the use or possession of the Deliverables (or any of the materials referred to at clause 29.1) does not infringe such Intellectual Property Rights.

31.2 The Service Provider must promptly notify the Purchaser if any claim or demand is made or action brought against the Service Provider for infringement or alleged infringement of any Intellectual Property Right which may affect the use or possession of the Deliverables (or any of the materials referred to at clause 29.1) or which may affect the provision of the Services.

31.3 Where a claim to which this clause applies is made, the Service Provider must, at its expense, use its best endeavours to:

31.3.1 modify the relevant Services or Deliverables or materials (as the case may be)or substitute alternative Services or Deliverables or materials (in any case without reducing performance or functionality) so as to avoid the infringement or alleged infringement of the Intellectual Property Rights; or

31.3.2 procure the grant of a licence or licences from the pursuer, claimant or complainer, on terms acceptable to the Purchaser, so as to avoid the infringement or alleged infringement of the Intellectual Property Rights of the pursuer, claimant or complainer.

31.4 The Service Provider must not without the consent of the Purchaser make any admissions which may be prejudicial to the defence or settlement of any claim to which this clause applies.

31.5 The Service Provider shall indemnify the Purchaser and hold it harmless from and against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Purchaser may suffer or incur as a result of or in connection with any breach of this clause 31.

32 Assignation

32.1 The Service Provider may not assign its interest in the Contract or any part of it without the prior written consent of the Purchaser.

32.2 Notwithstanding clause 32.1, the Service Provider may assign to another person (an "**Assignee**") the right to receive the price due to the Service Provider under the Contract subject to:

32.2.1 deduction of sums in respect of which the Purchaser exercises its right of recovery under clause 13 (Recovery of Sums Due); and

32.2.2 all the related rights of the Purchaser under the Contract in relation to the recovery of sums due but unpaid.

32.3 The Service Provider must notify or ensure that any Assignee notifies the Purchaser of any variations to the arrangements for making payments or for handling invoices, in each case in good time to enable the Purchaser to redirect payments or invoices accordingly. In the absence of such notification the Purchaser is under no obligation to vary its arrangements for making payments or for handling invoices.

32.4 Subject to clause 32.6, the Purchaser may assign, novate or otherwise dispose of its rights and obligations under the Contract or any part thereof to:

(a) any Contracting Authority; or

(b) any other body established by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Purchaser; or

(c) any private sector body which substantially performs the functions of the Purchaser,

provided that any such assignation, novation or other disposal shall not increase the burden of the Service Provider's obligations under the Contract.

32.5 Any change in the legal status of the Purchaser such that it ceases to be a Contracting Authority shall not, subject to clause 32.6, affect the validity of the Contract. In such circumstances, the Contract shall bind and inure to the benefit of any successor body to the Purchaser.

32.6 If the rights and obligations under the Contract are assigned, novated or otherwise disposed of pursuant to clause 32.4 to a body which is not a Contracting Authority or if there is a change in the legal status of the Purchaser such that it ceases to be a Contracting Authority (in the remainder of this clause both such bodies being referred to as the **"Transferee"**):

(a) the rights of termination of the Purchaser in clauses 57 (Termination Rights) and 58 (Termination on Insolvency and Change of Control) shall be available to the Service Provider in the event of respectively, the bankruptcy or insolvency, or Default of the Transferee; and

(b) the Transferee shall only be able to assign, novate or otherwise dispose of its rights and obligations under the Contract or any part thereof with the prior consent in writing of the Service Provider.

32.7 The Purchaser may disclose to any Transferee any confidential information of the Service Provider (including the Service Provider Sensitive Information) which relates to the performance of the Service Provider's obligations under the Contract. In such circumstances the Purchaser shall authorise the Transferee to use such confidential information only for purposes relating to the performance of the Service Provider's obligations under the Contract and for no other purpose and shall take all reasonable steps to ensure that the Transferee gives a confidentiality undertaking in relation to such confidential information.

33 Change of Control

The Service Provider must notify the Purchaser:

33.1 whenever it proposes to undergo a change of Control, or a change of control is likely to occur; and

33.2 immediately following a change of Control that has occurred.

34 Sub-Contracting

34.1 The Purchaser approves the appointment of the sub-contractors specified in Schedule 6 (Approved Sub-contractors) in respect of the obligations specified in that Schedule.

34.2 The Service Provider may not sub-contract its obligations under the Contract to other sub-contractors without the prior written consent of the Purchaser. Sub-contracting of any part of the Contract shall not relieve the Service Provider of any obligation or duty attributable to the Service Provider under the Contract. The Service Provider shall be responsible for the acts and omissions of its sub-contractors as though they are its own.

34.3 Where the Service Provider enters into a sub-contract the Service Provider must ensure that a provision is included which:

34.3.1 requires payment to be made of all sums due by the Service Provider to the sub-contractor within a specified period not exceeding 30 days from the receipt of a valid invoice as defined by the sub-contract requirements and provides that, where the Purchaser has made payment to the Service Provider in respect of Services and the sub-contractor's invoice relates to such Services then, to that extent, the invoice must be treated as valid and, provided the Service Provider is not exercising a right of retention or set-off in respect of a breach of contract by the sub-contractor or in respect of a sum otherwise due by the sub-contractor to the Service Provider, payment must be made to the sub-contractor without deduction;

34.3.2 notifies the sub-contractor that the sub-contract forms part of a larger contract for the benefit of the Purchaser and that should the sub-contractor have any difficulty in securing the timely payment of an invoice, that matter may be referred by the sub-contractor to the Purchaser;

34.3.3 requires that all contracts with subcontractors and suppliers which the subcontractor intends to procure, and which the subcontractor has not before the date of this Contract, already planned to award to a particular supplier are advertised through the Public Contracts Scotland procurement portal and awarded following a fair, open, transparent and competitive process proportionate to the nature and value of the contract; and

34.3.4 is in the same terms as that set out in this clause 34.3 (including for the avoidance of doubt this clause 34.3.4) subject only to modification to refer to the correct designation of the equivalent party as the Service Provider and sub-contractor as the case may be.

34.4 The Service Provider shall also include in every sub-contract:

34.4.1 a right for the Service Provider to terminate that sub-contract if the relevant sub-contractor fails to comply in the performance of its contract with legal obligations in the fields of environmental, social or employment law or if any of the termination events (involving substantial modification of the Contract, contract award despite the existence of exclusion grounds or a serious infringement of EU legal obligations) specified in clause 57.3 occur; and

34.4.2 a requirement that the sub-contractor includes a provision having the same effect as 34.4.1 in any sub-contract which it awards.

In this clause 34.4, '**sub-contract**' means a contract between two or more service providers, at any stage of remoteness from the Purchaser in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Contract.

34.5 Where requested by the Purchaser, copies of any sub-contract must be sent by the Service Provider to the Purchaser as soon as reasonably practicable.

34.6 Where the Service Provider proposes to enter into a sub-contract it must:

34.6.1 advertise its intention to do so in at least one trade journal, at least one newspaper circulating in Scotland and the Public Contracts Scotland Portal; and

34.6.2 follow a procedure leading to the selection of the sub-contractor which ensures reasonable competition following principles of equal treatment, non-discrimination and transparency and which ensures that such procedure is accessible by small and medium enterprises.

35 Change

Change Control Procedure

35.1 Any requirement for a Change shall be subject to the Change Control Procedure.

Change in Law

35.2 The Service Provider shall neither be relieved of its obligations to supply the Services in accordance with the terms and conditions of the Contract nor be entitled to an increase in the Contract Charges as the result of a Change in Law.

SECTION F SERVICE PROVIDER CONDUCT REQUIREMENTS

36 Compliance with the Law etc.

In providing the Services and otherwise when performing the Contract, the Service Provider must comply in all respects with:

36.1 all applicable Law;

36.2 any applicable requirements of regulatory bodies; and

36.3 Good Industry Practice.

37 Official Secrets Acts

The Service Provider undertakes to abide and procure that the Service Provider's employees abide by the provisions of the Official Secrets Acts 1911 to 1989.

38 Service Provider's responsibility for staff etc.

38.1 The Service Provider is responsible for the acts and omissions of all Service Provider Representatives relating to the Contract as though such acts and omissions are the Service Provider's own.

38.2 The Service Provider must ensure that all Service Provider Representatives:

38.2.1 are appropriately experienced, skilled, qualified and trained;

38.2.2 carry out their activities connected with the Contract faithfully and diligently and with all with due skill, care and diligence; and

38.2.3 obey all lawful and reasonable directions of the Purchaser when carrying out activities under the Contract.

39 Access to the Purchaser's premises

39.1 Any access to, or occupation of, the Purchaser's premises which the Purchaser may (at its discretion) grant the Service Provider from time to time is on a non-exclusive licence basis free of charge. The Service Provider must use the Purchaser's premises solely for the purpose of performing its obligations under the Contract and must limit access to the Purchaser's premises to such individuals as are necessary for that purpose.

39.2 The Service Provider must comply with the Purchaser's policies concerning Baseline Personnel Security Standard clearance and such modifications to those policies or replacement policies as are notified to the Service Provider from time to time.

39.3 At the Purchaser's written request, the Service Provider must provide a list of the names and addresses of all persons who may require admission to the Purchaser's premises in connection with the Contract, specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Purchaser may reasonably request.

39.4 The Service Provider must ensure that any individual Service Provider Representative entering the Purchaser's premises has completed the process for obtaining Baseline Personnel Security Standard clearance. The Service Provider acknowledges that the Purchaser has the right to deny entry to any individual that has not completed the process for obtaining Baseline Personnel Security Standard clearance.

39.5 In accordance with the Purchaser's policies concerning visitor access, entry to the Purchaser's premises may be granted to individual Service Provider Representatives for the purposes of meetings, notwithstanding that the process for obtaining Baseline Personnel Security Standard clearance has not commenced or completed.

39.6 The Purchaser may, by notice to the Service Provider, refuse to admit onto, or withdraw permission to remain on, the Purchaser's premises any Service Provider Representative whose admission or continued presence would, in the opinion of the Purchaser acting reasonably, be undesirable.

39.7 The Purchaser must provide advice and assistance acting reasonably to the Service Provider to facilitate the Service Provider's compliance with this clause.

39.8 All decisions of the Purchaser under this clause are final and conclusive.

40 Service Provider's Equipment

40.1 The Service Provider must provide all Equipment necessary to perform any required activities on the Purchaser's premises or otherwise necessary for the provision of Services.

40.2 But the Service Provider must not, without the Purchaser's approval:

40.2.1 bring Equipment onto the Purchaser's premises; or

40.2.2 leave Equipment on the Purchaser's premises.

40.3 Any Equipment brought onto the Purchaser's premises:

40.3.1 remains the property of the Service Provider; and

40.3.2 is at the Service Provider's own risk and the Purchaser has no liability for any loss of or damage to the Equipment unless the Service Provider is able to demonstrate that such loss or damage was caused or contributed to by the Purchaser's Default.

40.4 The Service Provider must keep all Equipment brought onto the Purchaser's premises in a safe, serviceable and clean condition. The Purchaser may at any time require the Service Provider to remove from the Purchaser's premises any Equipment which in the opinion of the Purchaser acting reasonably is either hazardous, noxious or not in accordance with the Contract and substitute proper and suitable Equipment at the Service Provider's expense as soon as reasonably practicable.

40.5 On completion of any required activities on the Purchaser's premises or at the end of a Working Day (as appropriate), the Service Provider must at its own expense:

40.5.1 remove all Equipment; and

40.5.2 leave the premises in a clean, safe and tidy condition, clearing away all rubbish arising out of the Service Provider's activities.

40.6 The Service Provider is solely responsible for making good any damage to the Purchaser's premises or any objects contained therein, other than wear and tear, which is caused by the Service Provider.

41 Purchaser Property

41.1 Where the Purchaser issues Purchaser Property to the Service Provider, the Purchaser Property remains at all times the property of the Purchaser.

41.2 The Service Provider undertakes the safe custody of the Purchaser Property and to that end must:

41.2.1 keep the Purchaser Property in good order and condition (excluding wear and tear);

41.2.2 comply with any particular security requirements communicated to the Purchaser in relation to the Purchaser Property;

41.2.3 use any Purchaser Property solely in connection with the Contract and for no other purpose; and

41.2.4 store the Purchaser Property separately and ensure that it is clearly identifiable as belonging to the Purchaser.

41.3 The Purchaser Property is deemed for the purposes of clause 41.2.1 to be in good order and condition when received by the Service Provider unless the Service Provider notifies the Purchaser otherwise within 5 Working Days of receipt.

41.4 The Service Provider must not:

41.4.1 modify or replace the Purchaser Property;

41.4.2 use the Purchaser Property as security for a loan or other obligation;

41.4.3 sell, or attempt to sell or part with possession of the Purchaser Property; or

41.4.4 allow anyone to obtain a lien over, or right to retain, the Purchaser Property.

41.5 The Service Provider licences the Purchaser to enter any premises of the Service Provider during Working Hours on reasonable notice to recover any Purchaser Property.

41.6 The Service Provider undertakes the due return of the Purchaser Property and as such is liable for all loss of, or damage to, the Purchaser Property (excluding wear and tear), unless such loss or damage was caused or contributed to by the Purchaser's Default. The Service Provider must notify the Purchaser promptly and, in any event within 2 Working Days, upon becoming aware of any defects appearing in or losses or damage occurring to the Purchaser Property.

42 Health and Safety etc.

42.1 While on the Purchaser's premises, the Service Provider must comply with the Purchaser's policies concerning health and safety and fire and such modifications to those policies or replacement policies as are notified to the Service Provider from time to time.

42.2 The Service Provider must immediately inform the Purchaser in the event of any incident occurring in the performance of its obligations under the Contract on the Purchaser's premises where that incident causes any personal injury or damage to property which could give rise to personal injury. The Service Provider must then promptly notify the Purchaser of that fact.

42.3 The Purchaser must promptly notify the Service Provider of any health and safety hazards which may exist or arise at the Purchaser's premises and which may affect the Service Provider in the performance of its obligations under the Contract.

42.4 The Service Provider must promptly make available its statutory health and safety policy statement to the Purchaser on request.

42.5 The Service Provider shall promptly notify the Purchaser of any health and safety hazards which may arise in connection with the performance of the Services (including any which occur on the premises of Service Provider Representatives).

42.6 The Service Provider shall notify the Purchaser immediately in the event of any incident occurring in the performance of the Services (including any incident which occurs on the premises of Service Provider Representatives) where that incident has caused any personal injury or damage to property or which could have caused personal injury or damage to property.

42.7 The Service Provider shall comply (and ensure that all Service Provider Representatives comply) with the requirements of the Health and Safety at Work Act etc.1974 and any other applicable Law relating to health and safety, which may apply in the performance of the Services.

42.8 The Service Provider shall ensure that its health and safety policy statement (as required by the Health and Safety at Work Act etc.1974) is made available to the Purchaser on request.

42A. Effective Procedures

42A.1 The Service Provider shall have sufficiently robust procedures in place at all times to minimise the risk that Service Provider Representatives could pose to Customers.

42A.2 The Service Provider shall ensure that in respect of any Service Provider Representatives who will come into direct contact with any Customers that the Service Provider (or relevant third party employer) has received, reviewed and is content with the terms of a basic disclosure certificate from Disclosure Scotland in respect of the relevant individual (with updated satisfactory certificates to be received and reviewed periodically throughout the employment of the relevant individual). If at any time, the provision of the Services requires

enhanced Disclosure Scotland security clearances / certificates the Service Provider shall be responsible for ensuring compliance with any such enhanced requirements.

42A.3 It shall be at the Service Provider's sole responsibility and cost to ensure that the necessary Disclosure Scotland security clearances / certificates are being complied with. The Purchaser shall have a right to audit the Service Provider's compliance with this clause at any time during the Contract Period.

43 Offences

43.1 The Service Provider must not commit or attempt to commit any offence:

43.1.1 under the Bribery Act 2010;

43.1.2 of fraud, uttering, or embezzlement at common law; or

43.1.3 of any other kind referred to in regulation 58(1) of the Public Contracts (Scotland) Regulations 2015.

43.2 In performing its obligations under this Contract, the Service Provider shall, and shall ensure that each of its sub-contractors shall, comply with the terms of the Modern Slavery Act 2015 and all applicable regulations and codes in force in relation thereto.

43.3 Breach of clause 43 is a material breach for the purposes of clause 57.1.3 (Termination Rights).

44 Tax Arrangements

44.1 Where the Service Provider is liable to be taxed in the UK in respect of consideration received under this contract, it shall at all times comply with the Income Tax (Earnings and Pensions) Act 2003 (ITEPA) and all other statutes and regulations relating to income tax in respect of that consideration.

44.2 Where the Service Provider is liable to National Insurance Contributions (NICs) in respect of consideration received under this contract, it shall at all times comply with the Social Security Contributions and Benefits Act 1992 (SSCBA) and all other statutes and regulations relating to NICs in respect of that consideration.

44.3 The Purchaser may, at any time during the Contract Period, request the Service Provider to provide information which demonstrates how the Service Provider complies with sub-clauses 44.1 and 44.2 above or why those clauses do not apply to it.

44.4 A request under sub-clause 44.3 above may specify the information which the Service Provider must provide and the period within which that information must be provided.

44.5 The Purchaser may supply any information which it receives under clause 44 to the Commissioners of Her Majesty's Revenue and Customs for the purpose of the collection and management of revenue for which they are responsible.

44.6 The Service Provider shall take all reasonable steps to ensure the observance of the provisions of this clause 44 by all of their servants, employees, agents, consultants and sub-contractors.

44.7 Where the Service Provider enters into any sub-contract with any of its servants, employees, agents, consultants and/or sub-contractors, the Service Provider must ensure that a provision is included which is in the same terms as this clause 44 subject only to modification to refer to the correct designation of the equivalent party as the Service Provider.

44.8 The Service Provider shall indemnify the Purchaser against any income tax, national insurance and social security contributions and any other liability, deduction, contribution,

assessment or claim arising from or made in connection with the provision of the Services by the Service Provider or any Service Provider Representatives.

45 Discrimination

The Service Provider must not unlawfully discriminate against any person within the meaning of the Equality Act 2010 in its activities relating to the Contract or any other contract with the Purchaser.

46 Blacklisting

The Service Provider must not commit any breach of the Employment Relations Act 1999 (Blacklists) Regulations 2010 or section 137 of the Trade Union and Labour Relations (Consolidation) Act 1992, or commit any breach of the Data Protection Act 1998 by unlawfully processing personal data in connection with any blacklisting activities. Breach of this clause is a material breach of the Contract which shall entitle the Purchaser to terminate in accordance with clause 57.1.3 (Termination Rights).

47 Sustainability etc.

47.1 The Service Provider must ensure that the Services are performed in accordance with the Scottish Government's environmental policy, which is to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone-depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment.

47.2 The Service Provider shall meet all requirements of the Scottish Government's sustainability policies, details of which can be found using website referred to below and which the Service Provider shall be deemed to be aware of:

http://www.scotland.gov.uk/Topics/Environment/SustainableDevelopment

48 Conflicts of interest

48.1 The Service Provider must take appropriate steps to ensure that the Purchaser is not placed in a position where, in the reasonable opinion of the Purchaser, there is an actual or potential conflict between the interests of the Service Provider and the duties owed to the Purchaser under the Contract.

48.2 The Service Provider must disclose by notice to the Purchaser full particulars of any actual or potential conflict of interest which may arise and must take such steps as are necessary to avoid or remove the conflict of interest.

48.3 Breach of this clause by the Service Provider is a material breach for the purposes of clause 57.1.3 (Termination Rights).

SECTION G FINAL PROVISIONS

49 Warranties and Representations

The Service Provider warrants and represents that:

49.1 it has full capacity and authority and all necessary consents (including where its procedures so require, the consent of its parent company) to enter into and perform its obligations under the Contract and that the Contract is executed by a duly authorised individual;

49.2 in entering the Contract it has not committed any offence under the Bribery Act 2010 or of fraud or uttering at common law or any other kind referred to in the Public Contracts (Scotland) Regulations 2015;

49.3 it has not committed any breach of the Employment Relations 1999 Act (Blacklists) Regulations 2010 or section 137 of the Trade Union and Labour Relations (Consolidation) Act 1992, or committed any breach of the Data Protection Act 1998 by unlawfully processing personal data in connection with any blacklisting activities;

49.4 as at the Effective Date, all information contained in the ESPD and Tender remains true, accurate and not misleading, save as may have been specifically disclosed in writing to the Purchaser prior to execution of the Contract;

49.5 no claim is being asserted and no litigation, alternative dispute resolution procedure or administrative proceeding is presently in progress or, to the best of its knowledge and belief, pending or threatened against it or any of its assets which will or might have a material adverse effect on its ability to perform its obligations under the Contract;

49.6 it is not subject to any contractual obligation, compliance with which is likely to have a material adverse effect on its ability to perform its obligations under the Contract;

49.7 no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Service Provider or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Service Provider's assets or revenue;

49.8 it owns, has obtained or is able to obtain, valid licences for all Intellectual Property Rights that are necessary for the performance of its obligations under the Contract;

49.9 in the 3 years prior to the Effective Date:

49.9.1 it has conducted all financial accounting and reporting activities in compliance in all material respects with the generally accepted accounting principles that apply to it in any country where it files accounts;

49.9.2 it has been in full compliance with all applicable securities and tax laws and regulations in the jurisdiction in which it is established;

49.10 it has not done or omitted to do anything which could have a material adverse effect on its assets, financial condition or position as an ongoing business concern or its ability to fulfil its obligations under the Contract;

49.11 it has made appropriate inquiries (for example as regards the Purchaser's premises) so as to be satisfied in relation to all matters connected with the performance of its obligations under the Contract;

49.12 it is familiar with the Purchaser's policies concerning Baseline Personnel Security Standard clearance and health and safety and fire as they apply at the Effective Date;

49.13 it has in place appropriate technical and organisational measures to safeguard any Purchaser Protected Information provided by the Purchaser;

49.14 there are no actual or potential conflicts between the interests of the Service Provider and the duties owed to the Purchaser under the Contract, save as may have been specifically disclosed in writing to the Purchaser prior to execution of the Contract; and it is deemed to have inspected any premises at which the services are to be performed as set out in the Specification (the 'Premises') before tendering so as

to have understood the nature and extent of the Services to be carried out and is deemed to be satisfied in relation to all matters connected with the Services and the Premises.

50 General Indemnity

The Service Provider shall indemnify the Purchaser against all claims, proceedings, actions, damages, costs, charges, expenses and any other liabilities which may arise out of, or in consequence of, any Default of the Service Provider.

51 Limitation of Liability

51.1 Subject to clause 51.2, neither Party is liable to the other Party under the Contract for any:

51.1.1 loss of profits, business, revenue or goodwill; or

51.1.2 indirect or consequential loss or damage.

51.2 Clause 51.1 shall not exclude any liability of the Service Provider for additional operational, administrative costs or expenses or wasted expenditure resulting from the direct Default of the Service Provider.

51.3 Subject to clauses 51.5 and 51.6, the aggregate liability of the Service Provider to the Purchaser for any one incident or a series of related incidents occurring in any Contract Year for Defaults under or in connection with the Contract shall in no event exceed 200% of the Contract Charges paid or payable in the relevant Contract Year in which the liability arises (on the basis that the Services had been properly performed) .

51.4 Subject to clause 51.6, the aggregate liability of the Purchaser to the Service Provider in any Contract Year for Defaults under or in connection with the Contract shall in no event exceed 100% of the Contract Charges paid or payable in the relevant Contract Year in which the liability arises.

51.5 The Service Provider's liability to the Purchaser under any of the following clauses shall be unlimited:-

51.5.1 clause 12.7 (Payment and Invoicing);

51.5.2 clause 14 (Data Protection Act);

51.5.3 clause 16 (Purchaser Protected Information);

51.5.4 clause 24 (Staff Transfer at Commencement);

51.5.5 clause 26 (Staff Transfer on Expiry or Termination);

51.5.6 clause 27 (Security)

51.5.7 clause 31 (Claims relating to Intellectual Property Rights);

51.5.8 clause 43 (Offences);

51.5.9 clause 44.8 (Tax Arrangements);

51.5.10 clause 45 (Discrimination);

51.5.11 clause 46 (Blacklisting); and

51.5.12 clause 49.1 and 49.2 (Warranties and Representations).

51.6 Neither Party excludes or limits liability to the other Party for:

51.6.1. death or personal injury caused by its negligence;

51.6.2. misrepresentation;

51.6.3. any breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or sections 2 or 11B of the Supply of Goods and Services Act 1982; or

51.6.4 any liability to the extent that it cannot be limited or excluded by Law.

52 Insurances

52.1 The Service Provider must effect and maintain with a reputable insurance company:

52.1.1 public liability insurance in the sum of not less than **twenty million pounds** (**£ 20,000,000)**;

52.1.2 professional indemnity insurance in the sum of not less than **ten million pounds** (**£ 10,000,000)** and

52.1.3 employer's liability insurance in accordance with any legal obligation for the time being in force.

52.2 Such insurance must be maintained for the Contract Period and for a minimum of 5 years following the expiry or termination of the Contract.

52.3 The Service Provider must give the Purchaser, on request, copies of all insurance policies referred to in this clause or a broker's verification of insurance to demonstrate that the appropriate cover is in place, together with receipts or other evidence of payment of the latest premiums due under those policies.

53 Force Majeure

53.1 Neither Party is liable to the other Party for any delay in performing, or other failure to perform, its obligations under the Contract to the extent that such delay or failure is a result of Force Majeure. Nonetheless, each Party must use all reasonable endeavours to continue to perform its obligations under the Contract for the duration of such Force Majeure. However, if Force Majeure prevents either Party from performing its material obligations under the Contract for a period in excess of 90 Days, either Party may terminate the Contract with immediate effect by notice.

53.2 Any delay or other failure by the Service Provider in performing its obligations under the Contract which results from any failure or delay by a Service Provider Representative is only to be regarded as due to Force Majeure if that Service Provider Representative is itself impeded by Force Majeure from complying with an obligation to the Service Provider.

53.3 If either Party becomes aware of Force Majeure which gives rise to, or is likely to give rise to, any delay or failure on its part as described in clause 53.1, it must immediately notify the other Party of the Force Majeure and the estimated period for which the failure or delay is to continue.

53.4 The only events that afford relief from liability for failure or delay under the Contract are Force Majeure events.

54 Dispute Resolution

54.1 The Parties must attempt in good faith to resolve any dispute between them arising out of or in connection with the Contract in accordance with the Management Arrangements.

54.2 Subject to clause 59.2, any dispute or difference arising out of or in connection with the Contract, including any question regarding its existence, validity or termination, which cannot be resolved in accordance with the Management Arrangements, shall be determined by the appointment of a single arbitrator to be agreed between the Parties, and failing agreement within 14 days after either Party has given to the other a written request to concur in the appointment of an arbitrator, by an arbitrator to be appointed by the Scottish Arbitration Centre on the written application of either Party. The seat of the arbitration shall be in Scotland. The language used in the arbitral proceedings shall be English.

54.3 Any arbitration under clause 54.2 is subject to the Arbitration (Scotland) Act 2010.

55 Severability

If any provision of the Contract is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision is severed and the remainder of the provisions of the Contract continue in full force and effect as if the Contract had been executed with the invalid, illegal or unenforceable provision eliminated.

56 Waiver and Cumulative Remedies

56.1 Any failure of either Party to insist upon strict performance of any provision of the Contract, or the failure of either Party to exercise, or any delay in exercising, any right or remedy does not constitute a waiver of that right or remedy and does not cause a diminution of the obligations established by the Contract.

56.2 Accordingly, no waiver is effective unless it is expressly stated to be a waiver and communicated to the other Party in writing in accordance with clause 10 (notices).

56.3 A waiver of any Default is not a waiver of any subsequent Default.

56.4 The rights and remedies provided by the Contract are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy is not to be deemed an election of such remedy to the exclusion of other remedies.

57 Termination Rights

57.1 The Purchaser may terminate the Contract by notice to the Service Provider with immediate effect if the Service Provider commits a Default and:

57.1.1 the Service Provider has not remedied the Default to the satisfaction of the Purchaser within 20 Working Days, or such other period as may be specified by the Purchaser, after issue of a notice specifying the Default and requesting it to be remedied;

57.1.2 the Default is not in the opinion of the Purchaser, capable of remedy; or

57.1.3 the Default is a material breach of the Contract; or

57.1.4 without prejudice to clause 57.1.1 to 57.1.3, the Default concerns the Service Provider's repeated or persistent failure to meet the Service Levels (or any of them).

57.2 The Purchaser may also terminate the Contract in accordance with any provisions of the Schedules which permit the Purchaser to do so.

57.3 The Purchaser may terminate the Contract in the event that:

(a) the Contract has been subject to substantial modification which would have required a new procurement procedure in accordance with regulation 72(9) (modification of contracts during their term) of The Public Contracts (Scotland) Regulations 2015;

(b) the Service Provider has, at the time of contract award, been in one of the situations referred to in regulation 58(1) (exclusion grounds) of The Public Contracts (Scotland) Regulations 2015, including as a result of the application of regulation 58(2) of those regulations, and should therefore have been excluded from the procurement procedure; or

(c) the Contract should not have been awarded to the Service Provider in view of a serious infringement of the obligations under the Treaties and the Directive 2014/24/EU that has been declared by the Court of Justice of the European Union in a procedure under Article 258 of the Treaty on the Functioning of the European Union.

In this Condition, 'the Treaties' has the meaning given in the European Communities Act 1972.

57.4 The Purchaser may also terminate the Contract in the event of a failure by the Service Provider to comply in the performance of the Services with legal obligations in the fields of environmental, social or employment law.

58 Termination on Insolvency and Change of Control

58.1 The Service Provider shall notify in writing immediately, and the Purchaser may terminate the Contract with immediate effect by notice, where in respect of the Service Provider:

58.1.1 a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignation for the benefit of, its creditors;

58.1.2 a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation);

58.1.3 a petition is presented for its winding up (which is not dismissed within 14 days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986;

58.1.4 a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets;

58.1.5 an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given;

58.1.6 it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986;

58.1.7 being a "small company" within the meaning of section 382 of the Companies Act 2006, a moratorium comes into force pursuant to schedule A1 to the Insolvency Act 1986;

58.1.8 a debt relief order is entered into; or

58.1.9 any event similar to those listed above occurs under the law of any other jurisdiction.

58.2 The Purchaser may terminate the Contract by notice with immediate effect within 6 months of:

58.2.1 being notified that a change of Control has occurred in accordance with clause 33.2 (Change of Control); or

58.2.2 where no such notification has been given, the date that the Purchaser becomes aware of the change of control.

58.3 But the Purchaser may not terminate the Contract under clause 58.2 where approval of the change of control has been granted by notice by the Purchaser.

59 Exit Management

59.1 The Service Provider shall comply with the provisions of Schedule Part 10 (Exit Management) and any current Exit Plan in relation to orderly transition of the Services to the Purchaser or the Replacement Service Provider.

59.2 The Service Provider agrees that if it breaches (or attempts or threatens to breach) its obligation to provide Exit Management, the Purchaser and their respective customers and stakeholders shall be irreparably harmed. In such circumstance, the Service Provider agrees that the Purchaser may proceed directly to court in accordance with clause 61 (Governing Law and Jurisdiction) notwithstanding anything to the contrary in the dispute resolution procedure outlined in Clause 54 (Dispute Resolution). If a court of competent jurisdiction finds that the Service Provider has breached (or attempted or threatened to breach) any such obligation, the Service Provider agrees that without any additional findings of irreparable injury, or other conditions to interdict, the Service Provider shall not oppose the entry of an appropriate order compelling performance by the Service Provider and restraining the Service Provider from any further breaches or attempted or threatened breaches of its obligations in relation to Exit Management.

60 Consequences of Expiry or Termination

60.1 Where the Purchaser terminates the Contract under clause 57 (Termination Rights) and makes other arrangements for the provision of services, the Service Provider indemnifies the Purchaser against all costs incurred in making those arrangements.

60.2 Where the Purchaser terminates the Contract under clause 5 (Break), the Purchaser indemnifies the Service Provider against any unavoidable losses directly resulting from the termination of the Contract.

60.3 The indemnity given by the Purchaser under clause 60,2 is subject to the Service Provider:

60.3.1 taking all reasonable steps to mitigate its loss;

60.3.2 taking all reasonable steps to recover its losses under any insurance policies held by it; and

60.3.3 submitting a fully itemised and costed list of losses which it seeks to recover from the Purchaser together with supporting evidence.

60.4 On expiry or termination of the Contract the Service Provider must:

60.4.1 immediately return to the Purchaser all Purchaser Property and Purchaser Protected Information in its possession; and

60.4.2 destroy or delete any copies of Purchaser Protected Information (whether physical or electronic) in its possession.

60.5 The following provisions survive the expiry or termination of the Contract:

60.5.1 clause 1 (Definitions and Interpretation);

60.5.2 clause 13 (Recovery of Sums Due);
60.5.3 clause 14 (Data Protection Act);
60.5.4 clause 15 (Freedom of Information);
60.5.5 clause 16 (Purchaser Protected Information);
60.5.6 clause 17 (Service Provider Sensitive Information);
60.5.7 clause 18 (Audit and Records Management);
60.5.8 clause 19 (Publicity);
60.5.9 clause 23 (Offers of Employment);
60.5.10 clause 25 (Information about Service Provider Employees);
60.5.11 clause 26 (Staff transfer on expiry or termination);
60.5.12 clause 28 (Parties' pre-existing Intellectual Property Rights);
60.5.13 clause 29 (Specially Created Intellectual Property Rights);
60.5.14 clause 30 (Licences of Intellectual Property Rights);
60.5.15 clause 31 (Claims relating to Intellectual Property Rights);
60.5.16 clause 37 (Official Secrets Acts);
60.5.17 clause 40 (Service Provider's Equipment);
60.5.18 clause 41 (Purchaser Property);
60.5.19 clause 44 (Tax arrangements);
60.5.20 clause 47 (Sustainability);
60.5.21 clause 49 (Warranties and Representations);
60.5.22 clause 50 (General Indemnity);
60.5.23 clause 51 (Limitation of Liability);
60.5.24 clause 52 (Insurances);
60.5.25 clause 54 (Dispute Resolution);
60.5.26 clause 56 (Waiver and Cumulative Remedies);
60.5.27 this clause 60; and
60.5.28 clause 62 (Governing Law and Jurisdiction).

60.6 If a Judicial Order is made, the provisions of the Management Arrangements referring to that possibility apply.

60.7 Immediately upon termination of the Contract for any reason whatsoever the Service Provider shall render such reasonable assistance to the Purchaser or third party nominated by the Purchaser, if requested, as may be necessary to effect an orderly assumption by a Replacement Service Provider of the Services previously performed by the Service Provider under the Contract. The Service Provider shall be entitled to charge for such termination services in accordance with Schedule 10 (Exit Management).

61 Entire Agreement

61.1 The Contract constitutes the entire agreement between the Parties in respect of the matters dealt with herein. The Contract supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral, except that this clause does not exclude liability in respect of any misrepresentation (whether in the ESPD or Tender or otherwise).

61.2 In the event of, and only to the extent of, any conflict between the clauses of the Contract, the Schedules and any document referred to in the Contract, the following order of precedence applies:

61.2.1 the clauses of the Contract;

61.2.2 Schedule 1 (Specification and Service Levels) and their Annexes;

61.2.3 any other Schedule Parts and their Annexes; and

61.2.4 any other document referred to in the Contract.

62 Governing Law and Jurisdiction

This Contract and any disputes or claims arising out of or in connection with its subject matter or formation (including non-contractual disputes or claims) is governed by and interpreted in accordance with Scots law and, subject to clause 54 (Dispute Resolution), the Parties submit to the exclusive jurisdiction of the Scottish courts over any dispute, claim or matter arising under or in connection with this Contract or the legal relationships established by this Contract (including non-contractual disputes or claims)..

IN WITNESS WHEREOF these presents typewritten on this and the 44 preceding pages together with the thirteen Schedules annexed are executed as follows:

SIGNED for and on behalf of the Scottish Ministers	**SIGNED** for and on behalf of PeoplePlus Group Limited
At.....	At.....
On.....	On.....
Signature.....	Signature.....
Full name	Full name.....
Position	Position.....
Address.....	Address.....
In the presence of	**In the presence of**
Signature.....	Signature.....
Full name	Full name.....
Address.....	Address.....

This and the following 77 pages comprise Schedule 1 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 1

SPECIFICATION AND SERVICE LEVELS

FOR

EMPLOYABILITY SUPPORT SERVICES

FAIR START SCOTLAND

Contents

1. Introduction and Purpose of Service 49
2. The Scottish Approach to Employment Support 50
3. Equalities 51
4. Customer Suitability and Eligibility 52
5. Service Requirement 56
6. Contract Lots 57
7. Service Strands 58
8. Segmentation Tool 58
9. Service Strand Description - Core Service Strand 59
10. Service Strand Description - Advanced Service Strand 60
11. Service Strand Description – Intense Service Strand 61
12. Customer Journey 62
14. Employer Engagement 70
15. Stakeholder Engagement Strategy 71
16. Service Provider Behaviours 72
17. Branding, Communications, Marketing and Accessibility 72
18. Feedback, Suggestions, Complaints and Escalation 73
19. IT 74
20. Innovation 75
22. Outcomes not eligible as Job Outcomes 77
23. Management Information 77
24. Performance Management 79
25. Tracking Period 80
26. Monitoring and Evaluation Activities 81
27. Assurance and Fraud Team Reviews 82
28. Continuous Improvement 82
29. Service Budget and Funding Model 82
30. Payment Validation Process 83
31. Key Delivery Indicators - Validation Process 83
32. Customer Travel Expenses 84
33. Childcare Costs 84
34. Additional Costs 84
35. Open Book Accounting 85
36. Contract Management and Key Contract Milestones Dates 85

37. Contract Extension 86
38. Contract Management 86
39. Contract Review Meetings 87
40. Change Control Procedures 87
41. Mobilisation and Implementation 87
42. Data Management 88
43. Exit Strategy 88
44. Business Continuity & Disaster Recovery 88
45. Physical Data Security 88
46. Storage of Data 89
47. Risk 89
48. Sustainability, Environmental and Community Benefits 89
Annexes to the Specification 91
Annex A to Schedule 1: Sources of Information 92
Annex B to Schedule 1: Service Guarantee 93
Annex C to Schedule 1: Lots 95
Annex D to Schedule 1: Customer Volumes & Contract Values 96
Annex E to Schedule 1: Key Performance Indicators 100
Annex F to Schedule 1: Key Delivery Indicators 101
Annex G to Schedule 1: Integration and Alignment with Other Scottish Government Services 105
Annex H to Schedule 1: Additional information on Supported Businesses 106

Annex I to Schedule1: Technical Response Under separate WORD document 106
Annex J to Schedule: Clarifications Under separate WORD document 107

1. Introduction and Purpose of Service

1.1 The Scottish Government invited tenders to deliver a new Scottish Employability Support Service, 'Fair Start Scotland', that provides support to disabled people and those at risk of becoming long-term unemployed to find and retain work.

1.2 From April 2017, the Scottish Government will implement services in line with the duty enabled by Clause 31 of the Scotland Act 2016 to provide employment support for disabled people and those at risk of long term unemployment.

1.3 As a result of these new devolved powers, the Scottish Government commissioned a one year transitional programme to support those Customers defined in the Scotland Act 2016 ("Customers"). Following the transition year, Fair Start Scotland ("the new Service") will commence from 3 April 2018.

1.4 This approach allowed the Scottish Government time to work collaboratively with stakeholders to design a new employability support service. The new Service will provide a coherent range of support that will respond flexibly to the individual needs of Customers and their employers. The Service will assist those who want to work and need help to enter and remain in work.

Designing the Scottish Employability Support Service

1.5 In summer 2015, the Scottish Government launched its consultation on devolved employability services, *Creating a Fairer Scotland: Employability Support*[1]. The aim of the consultation exercise was to draw upon the wealth of experience within Scottish communities, including the employer and provider networks to help shape future employability support in Scotland.

1.6 Following engagement with stakeholders and analysis of the consultation responses, the Scottish Government published its response: *Creating a Fairer Scotland: A New Future for Employability Support in Scotland*[2].

1.7 The Scottish Government's approach to employability is founded on the following values, underpinned by six key principles that are integral to creating a fairer Scotland.

Our Values

Value 1: Dignity and respect

Scottish Ministers are clear that Scotland's public services will be based on a culture of respect. We will have a social contract with the people of Scotland that states Scotland's public services will treat everyone with respect and dignity, and the public will treat staff providing those services in the same way. The Service will be an exemplar of this approach.

Individuals can expect to be treated with dignity and respect through each step of their journey into work.

Value 2: Fairness and Equality

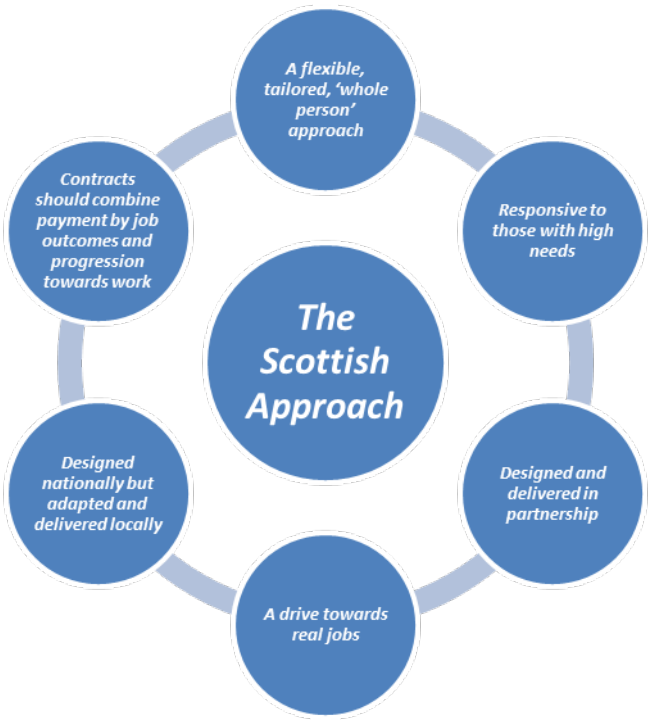
Our approach to employment support will not be driven solely by a need to reduce the Welfare Bill and focus on those with the best prospects of moving into work. Instead we will aim to contribute to a broader range of economic and social outcomes by supporting those furthest from the labour market. Customers of the Service will reflect this core value.

Value 3: Continuous Improvement

In the first instance, our priority will be to ensure a smooth transition from existing UK services to our new Scottish arrangements.

Scottish Government policies, processes and systems will evolve in response to individual, employer and community need across Scotland. The Scottish Government will ensure that they remain fit for purpose through close engagement with stakeholders and Service users alike.

Our Principles



1.8 The Scottish Government's expectation of how these values and principles can be delivered from 2018 Service is articulated through this specification. Service Providers must be clear how their provision will meet the specification and the Scottish Government's values and principles.

2. The Scottish Approach to Employment Support

2.1 The ambition to develop a distinctly 'Scottish Approach' to employment support received clear consensus and support through the 2015 consultation. The principles and values above provide the framework for this. In relation to this service requirement, the following service design elements and requirements on Service Providers are highlighted within the context of the 'Scottish Approach':

- All Customers who wish to access the Service will attend on a voluntary basis. Entirely voluntary participation creates the need for new and different relationships between referral organisations, Customers, Service Providers and Commissioners to ensure the service is both an attractive and successful support offer for Customers. The Scottish Government expects the Service Provider to be proactive in identifying, engaging and sustaining Customers in this context.

- The Service Provider will help to create a culture of dignity and respect within the Service. Having those values underpin their relationship with Customers will be the foundation on which this culture will be developed.

- All Customers must receive support which recognises their skills, attributes and assets, as well as their potential barriers to employment, with appropriate action taken to develop those individuals towards employment.

- The Service has been designed to allow the Service Provider the scope to develop personalised support for each Customer, based on their understanding of each individual and within the context of the most appropriate Service Strand for that individual. It is the responsibility of the Service Provider to build networks and align appropriate services to ensure each Customer receives the holistic support they require.

- The Scottish Approach will be underpinned by a jointly agreed Participation Agreement between the Service Providerand those participating in the Service, which will make clear the roles, responsibilities, expectations and obligations across both parties. This agreement will be underpinned by our commitment to guaranteed service levels – based on fairness, dignity and respect – and an appropriate personalised support offer.

- As the first full implementation of the Scottish Government's devolved powers on employment support, the need for continuous improvement both within the 2018 service and to inform future commissioning will be crucial and based on a partnership relationship between the Scottish Government and the Service Provider.

3. Equalities

3.1 The Scottish Government is clear in its ambitions to tackle inequality and a number of policies exist which it will be important to support through delivery of this Service.

3.2 **Disabled Employment:** At 40.9% the disabled employment rate is almost half of the non-disabled rate (81.5%) and is lower than the UK disabled employment rate of 47.9% (*ONS, Labour Force Survey, Apr-Jun datasets, 2016*)[3]. The Scottish Government has published a *Disability Delivery Plan*[4] with a series of key actions on employment and an overarching target to halve the disability employment gap. Devolved employment services will make a contribution to the achievement of this target. The Service sets out a clear focus on supporting disabled people into employment but will require the Service Provider to demonstrate a proven range of specialist skills and expertise to offer the individualised help many disabled people need to enter and sustain work.

3.3 **Women's Employment:** At first glance, women in Scotland perform well in the labour market. The current employment rate of 70.5% (ONS *Labour Force Survey June-August 2016*)[5] is the 4th highest in the EU and, since the 2008 recession, women have contributed significantly to the recovery of employment rates in Scotland – more so than in the rest of the UK.

3.4 However, occupational segregation continues to negatively affect women in terms of income levels. Caring responsibilities can mean that women tend towards lower skilled, lower paid jobs, often temporary in nature and the Scottish Government is keen to support actions to address the negative impact of such outcomes, which often lead to in-work poverty.

3.5 In line with Scottish Governments Fair Work ambitions, it is important for the Service Provider deliver a service that understands the support needs of women seeking employment. The Service Provider will use levers at their disposal to encourage employers to consider flexible working approaches which enable more women to take up a broader, more rewarding range of work opportunities. These must align with any caring responsibilities they have. The Scottish Government are seeking a gendered approach to employability support with the Service Provider supporting women into higher paid jobs in less traditional sectors.

3.6 **Black and Minority Ethnic (BME) Employment**: Some ethnic minority groups suffer disadvantage in the labour market, and when broken down by gender, the employment rate for women in these groups is even lower. There are many reasons for this. The Service Providermust engage positively to support such Customers into sustained employment, recognising the geographic variations in ethnic minority populations, and being sensitive to the cultural issues affecting them, particularly women and refugees.

3.7 **Other Protected Groups**: The Scottish Government lack robust evidence on how other protected groups are supported by employment services in Scotland and the outcomes they achieve. A clear ambition of the Service is to add to existing evidence and data on successful interventions for these groups.

4. Customer Suitability and Eligibility

Overview

4.1 Through delivery of this Contract, The Scottish Government is looking to support a minimum of 38,000 Customers' over 3 years of referrals. These Customers must be in receipt of a reserved UK out of work benefit, unless they are disabled, and will be either:

- aged 18 years old and over, out of work and living in Scotland; or
- aged 16 or 17 years old and are either disabled or in receipt of Employment and Support Allowance.

4.2 The Service will target:

- Disabled People (as defined in the *Equality Act 2010*[6]).
- Those who are long term unemployed (those reaching 2 years on Job Seekers Allowance/ Universal Credit equivalent).
- People on the Employment and Support Allowance Work Related Activity Group.
- People with convictions (someone who has completed a custodial sentence or a community sentence) or offender (someone who is completing a community sentence).
- Care Experience Young People.
- Lone Parents.
- Refugees.
- Ethnic Minorities.
- Resident in the 15% most deprived *Scottish Index of Multiple Deprivation (SIMD)*[7] areas.
- People with a health problem which presents a barrier to employment.

4.3 The Scottish Government reserves the right to amend the target Customer Groups during the term of the Contract to reflect any changes to its policies and/or priorities for employability support services in Scotland. Any amendments will be made following consultation with the Service Provider(s). Any such requirements will be subject to formal discussions and agreement according to the change control procedures detailed at Schedule 3 (Change Control Procedures).

Customer Suitability

4.4 The Service will support Customers who are significantly disadvantaged in the labour market and are assessed as having a realistic prospect of securing and sustaining work during their time on the Service.

4.5 For the majority of Customers, a realistic prospect of securing work is to be assessed by their potential to progress into work during the 12 months pre-work support period. However, for a minority of Customers, who are assessed as more disadvantaged in the labour market and

requiring additional specialist support to address their barriers, their pre-work period may be extended to 18 months with agreement from the Scottish Government.

4.6 All Customers who wish to access the Service will attend on a voluntary basis. However, Customers must be willing and able to attend regularly and engage positively with their Service Provider. The Customer and the Service Provider will agree the level and frequency of engagement during the Customer induction interview and profiling stages of the Service.

4.7 The Service will provide significant opportunities to support Customers who have a health condition and want to work. Customers will receive a range of specialised support to address the employability issues related to their health condition as described in the Service Strands requirements at paragraphs 10 and 11 of this specification.

4.8 All Customers must have their suitability for accessing the Service endorsed by their Referral Agency. Suitability must be determined by the Customer being eligible, having a realistic prospect of finding and securing work during their time on the Service, having an understanding of the Service, and being willing to engage.

4.9 The Scottish Government anticipate that the majority of Customers will be referred by Jobcentre Plus. These Customers will be identified by their Work Coach as needing more support than can be provided by the standard 'Jobcentre Plus Offer'. In all cases these Customers will have received the Jobcentre Plus core job search activity support without a successful outcome.

4.10 Additionally, other organisations operating in Scotland and supporting people who are disadvantaged in the labour market may wish to refer their clients to the Service as a next step following their own intervention. Alternatively, they may feel the Service is more appropriate for their Customers than their own support.

4.11 The *Employability Pipeline*[8] was developed in 2006 as a framework to support the effective delivery of employability services in Scotland. The Employability Pipeline sets out a 5 stage journey people may go through to enter and sustain work. The Employability Pipeline outlines the support they will require at each stage of the journey, although it also recognises that for some people, this is not a linear journey. The Scottish Government expect those referred to the Service to be in stages 2 - 4 of the Pipeline, with most being in stages 2 or 3 ('Needs Assessment and Barrier Removal' and 'Vocational Activity' respectively).

Offer to Disabled People

4.12 Disabled People, including those with severe and enduring mental health issues, will potentially access the Service, subject to suitability criteria, presenting with a wide range of issues. The Scottish Government requires specialised support to be put in place to meet all of their needs. The Service Provider must ensure that their delivery model offers a pan-disability service, offering high quality interventions for all Disabled People at all stages of their employment journey.

4.13 The Scottish Government anticipate that the majority of Disabled People will access either the Advanced or Intense Service Strands. In both these Strands, the Service Provider must offer a diverse menu of interventions appropriate to the nature of the Customer's disability. See paragraphs 10 and 11 of this specification for more information about the Service Strands.

4.14 All Customers in the Intense Strand will be taken through an individual programme of pre-work support that is consistent with the principles and practices of Supported Employment. A small number of Customers in the Intense Strand will follow the 5 stage model described in the *Supported Employment Framework for Scotland*[9], while others will be offered the most valuable elements of the model, or variations of it from a wide range of interventions. This must be discussed and agreed with the Customer.

Eligibility, Qualifying Benefits and Entry Point to the Service

4.15 Customers must be in receipt of a reserved UK out of work benefit unless they are disabled. The table below details the eligible Customer Groups, the qualifying benefits and entry point to the Service.

Customer Group	**Qualifying Benefit**	**Entry Point to Service**
Disabled People	Employment and Support Allowance (ESA); Jobseekers Allowance (JSA), Universal Credit (UC); Income Support (IS); "or no benefit at all but must be out of work".	Immediate
Health Issue placed in Work Related Activity Group	ESA, UC or Credits Only	On outcome of Work Capability Assessment.
Long Term Unemployed	JSA, UC or Credits Only	On reaching 2 years unemployed following commencement of contract.
Person with a conviction	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Care Experience Young People	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Lone Parents	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Refugees	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Ethnic Minorities	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Resident in the 15% most deprived Scottish Index of Multiple Deprivation (SIMD) areas.	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Unemployed but with a health condition which is a barrier to employment.	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.

4.16 The Service will initially focus help towards the target Customer Groups as they cross the relevant benefit duration threshold detailed in the above table. Should participation on the Service not meet minimum expected levels, the Scottish Government may consider extending the eligibility criteria to increase participation.

4.17 It is anticipated that the majority of referrals will come from Jobcentre Plus, who will confirm that a Customer's benefit entitlement meets the eligibility requirements for access to help through the Service through their on-going Work Coach interaction with Customers.

4.18 Customers who leave the Service during the twelve month pre-employment support period due to ill health may be re-admitted to the Service for the Balance of time. This will be at the discretion of the Service Provider taking into account the prospect of the Customer finding work during their balance of time on the Service (this measure is flexibly designed to avoid disadvantaging Customers with fluctuating health conditions).

4.19 Customers who leave the pre-employment stage of the Service early to take up work and subsequently leave for any reason will be entitled to re-join the Service for the Balance of time if the following conditions are met:

- The Customer left the job within their In-Work-Support period; and
- The Referral Agency and the Service Provider both agree that the Customers requires further support and has a realistic chance of securing new employment.

4.20 Customers whose job ends during the In-Work-Support stage of the Service will be entitled to receive support to find alternative employment up to the end of the 12 month In-Work Support period.

4.21 If the Customer moves out of Scotland and is currently within the Pre-Employment stage of the Service they are deemed to have left the Service. The Service Provider must take steps to exit the Customer, taking appropriate action as detailed within the Operational Guidance and referring to guidance regarding completion of a Leaver Plan.

4.22 If the Customer moves out of the original Lot Area to another Lot Area in Scotland and remains out of work, the existing Service Provider must continue to ensure arrangements are in place to continue to provide support to the Customer in the new Lot Area.

4.23 If the Customer is currently in work but moves out of the Lot Area to another Lot Area in Scotland, the existing Service Provider must continue to provide In-Work Support.

4.24 If the Customer is currently in work in Scotland and moves out of Scotland, but continues in the same employment, the existing Service Provider must continue to provide In-Work Support.

Service Requirement

Overview

4.25 The Service will deliver high quality employment support to targeted Customers' who want and need help to enter and remain in work.

4.26 The Service will provide Customers with pre-employment support for a period of up to 12 months, and In-Work support for a period of up to 12 months.

4.27 For Customers in the Intense Strand (see paragraph 11 of this specification), with significant barriers to employment, there will be the option to extend the duration of pre-employment support up to 18 months in agreement with the Scottish Government. Customers whose pre-employment support period is extended to 18 months will retain entitlement to 12 months In-Work support.

4.28 The Service will support Customers who face a range of barriers to employment: from those who may require skills, health or literacy and numeracy support; to those for whom complex barriers and/or disabilities require more specialised support to help them find and sustain employment.

4.29 The Service will be tailored to meet individual Customer needs. The Service will provide a voluntary and coherent range of specialist support that responds flexibly and effectively to meet the needs of individual Customers and their employers.

4.30 A key issue highlighted by respondents to the Scottish Government consultation on employability in 2015 was the need for a clear and consistent set of service standards that the Service Provider must deliver to every Customer.

4.31 The Scottish Government has produced guaranteed service standards (see Annex B, Service Guarantee) that set out the level of support that must be available to all Customers accessing the Service.

4.32 To support delivery of these Standards, Customers and the Service Provider must agree and sign a Participation Agreement. A template Agreement will be provided by the Scottish Government and the Service Provider must include as a minimum:

- an outline of the service offer available to the Customer;
- roles and responsibilities of both the Service Provider and Customer, setting out the commitments of each party information on the benefits of the Service;
- details of the Service Provider's complaints and feedback process, including how the Service Provider will ensure the voice of the Customer is recognised and valued in service delivery and demonstrate how this shapes provision going forward;
- information on the Service Provider's performance/success rates (which may include case studies); and
- details of the Service Provider's service delivery model and channels of engagement, and what the expected outcomes are from the Customers' perspective. The Service Provider must note that the Scottish Government requires minimum core hours for the Service to be Monday to Friday 0900 – 1700, except on statutory public holidays.

4.33 To ensure the Service offers the most effective support possible to Customers, a number of key features need to be integral to its delivery. The Service Provider must:

- demonstrate innovative approaches to working with those with more complex support needs;

- deliver support for the Customers to enable them to achieve their potential, whilst ensuring the Customer retains full choice and control over the support that they receive at all times, within the Service Strand to which they are allocated;

- ensure all elements of their agreed service are accessible across the whole Lot and provide the Guaranteed Service of support for Customers as outlined in Annex B;

- actively promote the new Service to potential Customers and Referral Agencies, promoting integration and alignment with local organisations and stakeholders to support the effective delivery of the Service;

- identify partner organisations to deliver specialist provision to meet the needs of the diverse Customer Groups and work closely with others, e.g. health and/or social care organisations, to identify Customers who may benefit from the Service;

- build strong links with local employers to encourage participation in the delivery of the Service;

- operate a quality feedback process for Customers and their employers throughout the Customer employment journey;

- promote the Scottish Government's ambitions around Fair Work, payment of the *Scottish Living Wage* [10] and support the Scottish Government's Diversity and Equality Policy [11] to supply chain/ consortia partners and the employers that they work with; and

- ensure that Service Provider staff and their supply chain are checked to the appropriate disclosure level. Advice should be sought from Disclosure Scotland if required.

5. Contract Lots

5.1 The Service will be delivered across nine (9) geographical Lots based on clusters of Scottish Local Authority Areas. This offers a mix of viable contract sizes which the Scottish Government has awarded to a diverse range of Service Providers.

5.2 In line with Regulation 21 of the Public Contracts Scotland Regulations (2015), Scottish Ministers decided to reserve one Lot for supported businesses. The Scottish Government is committed to furthering the development of supported businesses in Scotland.

5.3 A Supported Business is defined in the Public Contracts (Scotland) Regulations 2015 as:

> *"an economic operator whose main aim is the social and professional integration of disabled or disadvantaged persons and where at least 30% of the employees of the economic operator are disabled or disadvantaged persons;"*

5.4 Lot: 'West' (covering the East Dunbartonshire, East Renfrewshire, Inverclyde, Renfrewshire and West Dunbartonshire Local Authority areas) is reserved.

5.5 All references to Lot: 'West' in this Specification are for information purposes only.

5.6 A single contract was awarded for each Lot. Further information about the Lots are included at Annexes C and D to this Schedule.

5.7 The Service must be available and accessible to all Customers living in the Lot. The Service Provider will be required to deliver the proposed provision from premises located within the relevant Lot. Customers will be resident in various areas across each Lot and so the delivery

premises should be sited in locations which are accessible via public transport. The Service Provider will be required to provide details of proposed delivery premises, including a rationale in support of their proposals.

6. Service Strands

6.1 The Service offer to Customers will be categorised by one of three Service Strands. The Scottish Government will provide a standardised Segmentation tool to assist in determining the Service Strand required by each Customer.

7.2. The assignment to the Core, Advanced or Intense Service Strands, as described below, will determine the level of support available to the Customer during their employment journey.

- **Core Service Strand** – for Customers who require a range of support to overcome barriers to work;

- **Advanced Service Strand** – for Customers who face more significant barriers to work and require specialist interventions and support; and

- **Intense Service Strand** – for Customers with multiple and more complex needs, and significant barriers to work, that require the support of dedicated specialist organisations.

7.3. The Service offer within each Strand is driven by the primary relevant barriers and the expected target Customer groups. However, the Service offer must be personalised and tailored to the needs of the individual Customer.

7.4. In line with the Scottish Government's core values, Customers, Service Provider staff, Consortium and/or Supply Chain partners and Stakeholders must always be treated with dignity and respect. As such, the Service Provider must refrain from using the Service Strand terminology or jargon with Customers.

7. Segmentation Tool

7.1 The Scottish Government wishes to ensure that every Customer is allocated to the Service Strand which provides the level and intensity of support that their barriers to employment require. It is anticipated that the Service Strands will therefore have different financial values to recognise the escalating need across the Customer groups.

7.2 The only purpose of this tool is to assign Customers who have voluntarily agreed to join the Programme to one of three Service Strands. The three Strands are:

a) Core
b) Advanced
c) Intense.

7.3 The Segmentation tool is *not* a full diagnostic of the needs of the Customers nor is it intended to be.

7.4 Every Customer who starts on the Programme must have completed the Segmentation Tool to determine the level of their needs and barriers to employment. It will be the responsibility of each Service Provider to ensure that every Customer has completed this activity in advance of starting on the Service.

7.5 The Service Strands are therefore a key driver of both the nature of the support given to a Customer and for the performance of the Programme (as measured by job outcomes). Making sure each Customer is assigned to the correct Strand will be critical to the success of the Service.

7.6 The Scottish Government is currently developing this tool and will 'test' this model prior to the Service commencement date. The Scottish Government will work closely with the Service Providerto ensure it operates correctly.

8. Service Strand Description - Core Service Strand

8.1 It is anticipated that Customers in this group will mostly be unemployed and job seeking and will be a mix of some Customers in the early entry categories (namely, Lone Parents, Care Leavers etc.) and some who have reached the 24 months unemployed stage. They will face barriers to work which might include a skills deficit, literacy and numeracy problems, and a lack of confidence and resilience. They may also face some 'environmental' barriers such as travel and childcare. The Scottish Government do not expect most of those with a disability or a health condition acting as a barrier to work to be in this Service Strand.

8.2 The Service Provider must provide Customers with a dedicated advisor and a range of activities that are tailored to individual Customers and their needs. The activities must build on the service outlined in the Guaranteed Service Standards. The level of activity and engagement will increase steadily during the time on the Strand to prepare the Customer for the world of work.

8.3 The level of activity and rate of increase in hours must be determined, agreed and recorded by the Service Provider and the Customer, and must recognise any benefit conditionality. Operational Guidance will provide further detail.

8.4 The Service Provider is encouraged to propose innovative delivery proposals for enhancing the Customer experience during this phase. Given the voluntary nature of the Service, Customers will need to be enthused to engage on a regular basis. The Service Provider may want to consider some form of Group activity that promotes collaborative engagement with Customers.

8.5 Detailed below are support activities that must be offered to Customers in this Strand. This is not an exhaustive list, and the Service Provider must determine the range of support available to reflect Customer needs:

- a mix of **one to one support and group work** with the expectation that individual's progress to intensive job search at an early stage. Depending upon Customer need, group work may include activities that promotes team-building; and develop the skills/attributes required in the workplace (e.g. interpersonal skills, communication skills, leadership skills etc.);

- **core employability support** from a dedicated adviser that builds upon services/interventions already received by the Customer from JCP or other specialist employability organisations (e.g. confidence/resilience building, preparing for interviews, job matching and brokerage);

- **employer presentations** – presentations from local employers about working in specific employment sectors e.g. retail, hospitality, business admin and manufacturing. This may cover how to get a job in a particular sector, application processes, recruitment practices (e.g. on-line job applications and questionnaires/psychometric testing etc.);

- **intensive job search**, including digital job search techniques, and the use of the internet/registrations with job sites/agencies etc.;

- **job application support** – including CV and interview preparation, skills development, managing disclosure of health/disability/conviction information, and advocacy to the employer if needed;

- **personal development** – improving self-esteem, addressing any issues with confidence, motivational, resilience and attitude;

- support from **a mentor**;

- **vocational or employability skills training** appropriate to Customer's job aspirations where it would remove a barrier to work;

- **volunteering** opportunities;

- **work experience/placements** – short work experience/placement opportunities with employers; these are expected to last between 4-6 weeks. This type of activity must recognise any benefit conditionality requirements; and

- support for Customers wanting to enter **self-employment**.

9. Service Strand Description - Advanced Service Strand

9.1 It is anticipated that these Customers will be a mix of; long term unemployed joining the service at 24 months; a smaller number of early entry unemployed people (for example Lone Parents, Care Leavers etc.); some disabled people and those in the Employment and Support Allowance Work Related Activity Group. In addition to the range of possible barriers faced by those in the Core Strand, they will possibly face a number of additional challenges. These might include: a long-term health problem which is acting as a barrier to work; in recovery from addictions; a record of convictions and/or other non-employability related issues, such as housing difficulties.

9.2 The Service Provider will provide Customers in this Strand with all appropriate support available to those in the Core Strand. In addition further specialist support such as is listed below must be available. This list is not exhaustive.

- **Access to specialist support to address health problems**. This must include professional help to manage mental/physical health conditions and well-being interventions. The Service Provider may wish to make Cognitive Behaviour Therapy or other forms of condition management available;

- **Support to find work while in recovery from drug/alcohol/substance misuse;**

- **Support to develop skills for the workplace**; and

- **Support to address the barriers faced because of a record on convictions.** This may include guidance on matters of disclosure.

9.3 It is the responsibility of the Service Provider to build networks and align appropriate services for each Customer to ensure they receive the holistic service they require as set out earlier in this document. The Scottish Government anticipate that this will be particularly applicable to those Customers in the Advanced Strand.

9.4 Therefore, in addition to the services above, and the specific needs of the Customer, the Service Provider may signpost/make a warm referral to other agencies and Scottish Government funded programmes where agreed with the funding body, including areas such as addiction services, housing support and childcare advice. Access to these initiatives is subject to a range of criteria and will, in some cases, be limited by the availability of places. The Service Provider is expected to negotiate with other local organisations to allow Customers to access these initiatives, if appropriate.

9.5 Some Customers who have a disability will be assessed as not requiring the high level of support available through the Intense Service Strand, and instead will be supported in the Advanced Strand. The Service Provider will have knowledge of their Customers with a disability and their likely barriers to employment. The Scottish Government would expect that:

- Disabled Customers in the Advanced Strand can expect to receive high quality, personalised one-to-one support with specialist provision where required;

- Disabled Customers will receive high quality assessment and action planning (although not necessary a full Vocational Profile); and

- Disabled Customers in the Advanced Strand must also receive Job Analysis, high quality In-Work Support and have an In-Work Action Plan.

9.6 The Scottish Government expect the level of activity and engagement to increase steadily during the time on the Strand to prepare the Customer for work. The level of activity and rate of increase in hours will be determined between the Service Provider and the Customer.

10. Service Strand Description – Intense Service Strand

10.1 It is anticipated that this Customer group will predominantly be disabled people. Others with long-term health conditions such as severe and enduring mental health conditions may not consider themselves disabled but may be judged by the Segmentation Tool as requiring this Intense Strand of support.

10.2 Others who face multiple and complex barriers to work may require this level of support. They are likely to have a poor or limited employment history, or have been out of work for 5 years or more and will face a range of barriers to work noted in the Core and Advanced paragraphs of this Schedule in addition to a disability and / or long-term health condition.

10.3 The service will be built on the principles of the Scottish Government Supported Employment Framework, and although not all Customers will follow the Framework, they can all expect a service including key elements of supported employment:

- All Customers will receive end to end and 1:1 support from a specialist key worker who has a sound knowledge of their disability and their barriers to employment.

- The Service Provider is required to ensure that staff involved in the delivery and management of this proposed support are appropriately qualified and/or experienced in delivery of Supported Employment services. The Service Provider is, therefore, required to provide information about the qualifications and experience of staff, together with an explanation of why they believe these to be appropriate in the context of the proposed provision.

10.4 All Customers must be offered Vocational Profiling, conducted to the best standard principles of person-centred planning and also include information on skills, attributes, aspirations, past experience, health and social issues, communication needs and how support will be delivered. This will be used to develop an action plan which will detail the activities to be carried out to prepare the client for employment.

10.5 Those in the Intense strand will require an enhanced level of support and there is an expectation that Customer to advisor ratios will be much lower in this group. It is recognised that there are practical challenges around setting a Key Delivery Indicator for this against which the Service Provideris measured, but evidence has shown that a Customer to Advisor ratio of 1:20 is appropriate. Independent advocacy support must be arranged where the Customer requests this.

10.6 The Service Provider must provide a range of activities that are tailored to individual Customers and their needs. The activities must build on the service outlined in the Guaranteed Service Standards. The Scottish Government expect the level of activity and engagement to increase steadily during the time on the Strand to prepare the Customer for

work. The level of activity and rate of increase in hours will be determined between the Service Provider and the Customer.

10.7 The Service Provider is expected to provide Customers in this Strand with all the support provided to those in the Core and Advanced Strands. In addition, the Service Provider will provide the following to the Customers in the Intense Strand (as before, this is not an exhaustive list) and the Service Provider must determine the range of support available to reflect Customer needs:

- Models including the Supported Employment Model for disabled people and Individual Placement and Support (IPS) for those with severe/enduring mental health challenges must be available and offered where required.

11. Customer Journey

11.1 The Scottish Government does not wish to be overly-prescriptive in terms of service content as this must be tailored to each Customers individual circumstances, their job aspirations and the needs of the local labour market. However, the Service Provider must follow the high level Customer Journey Stages set out in this specification.

11.2 Additionally, the Service Provideris required to observe and comply with any Operational Guidance which is issued by or on behalf of the Scottish Government during the Contract period. This guidance will be limited to administrative matters and will be considered for commercial impact on the Service Provider before issue. Where a change is considered significant it will be subject to discussion with Service Provider and subject to formal Change Control (see Schedule 3 (Change Control Procedures)) where the Service Provider considers this necessary.

11.3 Existing support funded through the Scottish Government to support skills development has been considered and Annex G sets out how the Service will align with these initiatives.

Stage 1: Pre Start – Identification and Referral

The Scottish Government anticipate the Service will attract referrals from a wide range of organisations across Scotland such as:

- Jobcentre Plus (JCP);
- Local Authorities;
- Third Sector organisations;
- Social Service Teams;
- Carer Groups;
- Education & Learning institutions; and
- The National Health Service / Health Scotland.

This list is not exhaustive.

The Referral Agency will provide the Customer with a brief overview of the Services offered by the Service Provider, the features and benefits of the Service, what support is available, and the location of the Service Provider's local offices. The Service Provider will provide their own marketing material to assist Referral Agencies with this step (see paragraph 17 for further information).

The Referral Agency should ensure the Customer's suitability for accessing the Service is agreed with the Customer prior to the Stage 2: Eligibility Check.

Stage 2: Eligibility Check

It is anticipated that JCP will be a primary source of referrals, and that all Customers in receipt of working age benefits, will have their eligibility checked via their on-going interaction with their JCP Work Coach, using the Service eligibility criteria, before being referred to the Service.

In instances where a referral is made to the Service Provider for Customers in receipt of working age benefits by an organisation other than JCP, the Service Provider must signpost the Customer back to JCP to ensure that the Customer's Work Coach actions the referral to the Service.

In a small number of cases, there may be eligible Customers for Fair Start Scotland who have no requirement to engage with Jobcentre Plus, either as they are not in receipt of benefit or their benefit conditionality does not require this. For this Customer group, a clerical referral can be made by the Referral Agency direct to the Service Provider, who will check eligibility. Details must be recorded in the Customer case file to confirm this action has been undertaken.

Full details of these processes will be shared through the Operational Guidance.

Stage 3: Referral Process and Warm Handover

The Scottish Government recognises that the ability to support warm handovers will depend on local arrangements, and relationships built between the Service Provider and their range of Referral Agency partners.

Where warm handovers can be supported, the Referral Agency will be responsible for contacting the Service Provider to arrange a 'warm handover' for the Customer. The Referral Agency, with the Customer's consent, will contact the Service Provider to discuss the referral details and Customer circumstances in advance of the warm handover.
The purpose of the warm handover is to:

- encourage effective working between the Referral Agencies and the Service Provider;
- improve the standard of referrals, in terms of appropriateness of referral and background information provided;
- establish the Customer's willingness to engage with the Service;
- enable a collective assessment between Customer, Referral Agency and Service Provider of the support needs of the individual; and
- agree a start date with the Customer to commence the Programme.

The warm handover meeting, attended by the Customer, Service Provider and Referral Agency, is expected to last up to 1 hour. The Customer must be made aware of the purpose and content of the meeting in advance of attending.

Preferably, the warm handover will be done face-to-face but it may be completed by telephone, Skype, etc. depending on local arrangements agreed with the Service Provider and the Referral Agency. Any travel costs incurred by the Customer will be the responsibility of the Service Provider.

At this stage the Customer may deselect themselves from further involvement in the Service. The Service Provider must notify the Referral Agency that the Customer has declined the offer of support.

The Service Provider will not have the option to reject referrals. Information about how to advise the Scottish Government of inappropriate referrals will be included the Operational Guidance.

Once the Customer agrees to engage with the Service, the Referral Agency will make a referral to the Service Provider. This is the date at which the Customer is referred to the Service. The Service Provider must confirm with the Referral Agency that the Customer has agreed to commence the Service and confirm their start date.

The Service start date and time (i.e. the induction interview appointment) must be no more than 5 working days, following receipt of the referral by the Service Provider. In exceptional circumstances and due to reasons out with the Service Providers control where this timescale cannot be met, the Service Provider must annotate the Customer file accordingly explaining the reason for the delayed start.

Stage 4: Pre Start

Immediately following the warm handover, the Service Provider must notify the Customer and Referral Agency in writing of the date and time for their Induction Interview, and follow up with a courtesy telephone call 48 hours prior to this appointment to alleviate any Customer concerns.

Prior to their Induction Interview with the Service Provider, the Customer must complete a Self-Assessment to determine the most suitable Service Strand for them. Should the Customer need help to complete the Self-Assessment, the Referral Agency should arrange this support.

The Self-Assessment will be undertaken by using the Segmentation Tool.

Stage 5: Service Start - Customer Induction Interview

The Service Provider has the discretion to determine the most appropriate format for managing and delivering Customer Induction Interviews. The only stipulations are that the interviews must be conducted face-to-face and within 5 working days of the initial Customer referral being received. If the Customer is unable to 'start' on the date offered, the Service Provider must record on file.

The purpose of the Induction Interview is to:

- outline the service offer;
- outline the roles and responsibilities for both the Service Provider and Customer and jointly sign a Participation Agreement, setting out the commitments of each party;
- introduce the Customer to their named key worker who will be responsible for providing continuity of support throughout the employment journey;
- provide an initial assessment to inform the Customer Profiling and Planning Stage (see Stage 6) of the Service; and
- discuss Customer participation in evaluation activities.

At the Induction Interview, the Service Provider must provide each Customer with an Induction Pack. As a minimum, this must include:

- Background of the Service Provider;
- What the Service offers;
- What happens next;
- Who are the Customer's key contacts;

- Details of Service Provider's Customer Charter and Complaints/ Suggestions procedures;
- Health and Safety requirements; and
- Other useful information – website details, success stories, information security, etc.

The Service Provider is encouraged to propose innovative delivery proposals to support and retain the commitment from the Customer. This must enhance the Customer experience throughout their participation on the Programme. Given the voluntary nature of the Service, Customers will need to be enthused to engage on a regular basis. The Service Provider will want to consider some form of group activity that promotes collaborative engagement with Customers from initial engagement through their time on the Programme.

The Service Provider must facilitate immediate referral to specialist services following the induction interview for Customers identified as having complex and significant barriers to work who require support provided through the Intense Service Strand. The specialist services organisations will be responsible for undertaking the Customer profiling and assessment activities.

Stage 6: Customer Profiling and Planning Activities (Week 1 to 8)

Once the Customer starts on the Programme, the Service Provider will undertake profiling and planning activities. The activities will be split into two parts:

Weeks 1 to 3

During the first three weeks the Service Provider must engage with the Customer to:

- assess their needs, identify barriers and job aspirations;

- review their completed self-assessment to confirm the service strand they will access; and

- confirm the level of support offered to the Customer determined by the appropriate Service Strand.

Weeks 4 to 8

The Service Provider will use the balance of time during this Stage of the Service to confirm the appropriateness of the allocation to the Service Strand.

There may be instances where the Service Provider considers that the original allocation to the Service Strand is wrong and, following observations and discussions during the activities outlined above, wishes to change the Service Strand. In exceptional circumstances and with the agreement of the Scottish Government a change to Service Strand may be approved. The process for this will be outlined in the Operational Guidance.

During this period the Service Provider must offer the following:

- Weekly interventions with the Customer's key worker;

- Access to a range of essential activities that will help to determine/confirm the level of help and support required, including but not limited to:

    - baseline development of employability skills;

    - health and well-being assessments and guidance;

    - jobsearch skills and resources;

- labour market information, including employer engagement;
- mentoring support;
- money management;
- personal development and soft skills training, e.g. communications and interpersonal skills;
- promotion of IT for job search (including assessment of IT skills);
- social activity to support the engagement and development of soft skills;
- understanding the world of work – employer presentations; and
- volunteering opportunities.

- development of a detailed personalised Employment Action Plan which sets out agreed activities and timescales for helping Customers into work. This will include: an assessment of current skills; employment history, vocational training needs; employment aspirations; agreed activities for overcoming barriers to employment, including engagement with external services; and monitoring and review arrangements and In-Work Support plan;
- identification, referral and support for the Customer to engage with specialist organisations to provide appropriate support to address issues;
- the opportunity to fast-track Customers to specialist organisations to provide appropriate support; and
- Customers with the highest support needs (i.e. those referred to the Intense Strand) will receive a Vocational Profiling service that supports their individual Action Plan during this period.

The Service Provider is required to propose innovative delivery proposals for enhancing the Customer experience during this phase.

Stage 7: Intervention and Customer Engagement (Weeks 9 to 52)

By week nine, Customers will commence in one of the three Service Strands. The Customer will continue to receive a range of core activities (listed at Stage 6), supplemented by more targeted and/or specialised interventions that address their needs and employability issues. The level of activity and engagement must increase steadily during the time on the Strand to prepare the Customer for the world of work.

To support the Guaranteed Service, the Service Provider must provide the following support during this stage of the employment journey:

- minimum of 3 hour face-to-face contact with named key worker per week;
- 1 to 1 coaching by the named key worker, as necessary;
- formal face-to-face monthly review with the named key worker;
- quarterly distance travelled assessment and feedback with the named key worker;
- employability activities as detailed in the individual Employment Action Plan;

- engagement with external, specialist or partner services as detailed in the individual Employment Action Plan;

- access to work experience opportunities and appropriate monthly workplace reviews;

- weekly job search activities;

- employer engagement, including support for interviews and negotiations of reasonable adjustments; and

- financial guidance.

Evidence of pre-employment activity and support must be recorded in individual Customer files and Action Plans which will form part of the monthly performance management process between the Service Provider and the Scottish Government.

If a job outcome is not achieved during this timeframe, the Service Provider will produce a Leaver Plan and refer the Customer back to the original Referral Agency.

In exceptional circumstances and due to unacceptable Customer behaviour, a process will be established to exercise an option to cease provision of Services. This process will be fully outlined within the Operational Guidance.

Service Provider Case Conferencing with Referral Agency

- It is considered good practice for the Service Provider to maintain contact with the Referral Agency to provide regular updates on those Customers they have referred to the service. Scottish Government would encourage arrangements to be put in place for Case Conferencing where appropriate to discuss the Customer's progress. These will mainly be done on an individual basis face to face or by conference call. These can also be conducted as part of a wider group session where deemed appropriate by the Service Provider and the Referral Agency.

Disengagement

- If the Customer disengages or becomes inactive, e.g. fails to attend appointment or participate in an agreed activity without prior notice, the Service Provider must contact the Customer within 24 hours to establish the circumstances surrounding the disengagement.

- If the Service Provider is unable to engage with the Customer within 5 working days of them failing to attend an appointment/activity they must contact the Referral Agency to ascertain the circumstances for this (focusing on known barriers and/or risks) and agree an appropriate way forward to re-engage the Customer.

- If the Customer disengages or becomes inactive on 3 separate occasions it is for the Service Provider to determine whether the Customer should continue to participate in the service. Service Providers are responsible for determining the most appropriate course of action. Full details of this process will be contained within the Operational Guidance.

- Should the Customer be dismissed from the Service, the Service Provider must record the reasons for dismissal within the Customer's Leaver Plan.

Stage 8: Customer does not find work during the 12 month pre-employment support period (Intense Service Strand Customers' only)

Only Customers in the Intense Service Strand who fail to secure employment following completion of the 12 month pre-employment support period may have the option to extend the pre-employment support. This can be extended to a maximum duration of 18 months, where Customer and Service Provider are agreed that there is a realistic prospect of the Customer finding a job in this timescale. Customers whose pre-employment support period is extended to 18 months will retain entitlement to 12 months In-Work support.

If there is no, or limited prospects of the Customer finding work within the 6 month extension period, the Service Provider must engage with the Referral Agency within 10 Working Days of Customer's end date to arrange for the Customer to be referred back. This is to ensure a smooth transition back to the Referral Agency and must be supported with a detailed Leaver Plan (in accordance with stage 9 below).

Stage 9: Service Exit and Leaver Plan

Customers failing to secure employment within 12 or 18 months (see stage 8 above re extensions) will be referred back to the Referral Agency responsible for the original introduction. The Service Provider must contact the Referral Agency prior to the Customer's end date to alert them that the Customer will be returning.

The Service Provider must produce a detailed Leaver Plan for each Customer returning to their Referral Agency. As a minimum, the Leaver Plan must include the following:

- identified barriers to employment, for example: addiction; and/or vulnerability issues;
- distance travelled, for example: new learning; basic skills; and learning and development activities;
- activities undertaken whilst on the Service;
- reason for leaving provision; and
- recommendations on next steps to support Customer move closer to employment.

The exit process and Leaver Plan applies to all Customers disengaging from the Service and returning to their Referral Agency. Those who, for any reason, do not enter work but do not complete the Programme, will be referred back to their Referral Agency for consideration of further support.

Stage 10: In Work Support (13-24 months, or job entry date + 12 months)

Once a Customer has found paid employment (or self-employment), the Service Provider will work with the employer and Customer, as appropriate and determined by the Customer, to identify the support required for the Customer to start and retain work. Thereafter the Service Provider will provide a period of In Work Support, which has the ambition of supporting job retention/ progression in terms of skills and / or income. Careers Information Advice and Guidance may be suitable at this stage.

In line with the funding model, the Scottish Government would not expect the total period of In Work Support to exceed 12 months.

The Service Provider will need to be fully conversant with the range of support that can be made available, and this information must be detailed within the Customer's In Work Support Plan.

Subject to the Customer's agreement, the Service Provider is required to support them to retain employment or secure new employment in the event of the Customer becoming unemployed before the 12 months in-work support period is complete.

The Service Provider is required to:

- facilitate within 10 working days of job start date, a jointly agreed In-Work Support Action Plan, detailing timeline for workplace reviews with employer, future training and career development goals and actions;
- support the workplace induction;
- provide a minimum of weekly contact with the Customer fading as appropriate;
- conduct monthly workplace reviews with the employer, reducing over time as appropriate;
- support at workplace training (if necessary);
- provide support to develop workplace relationships;
- provide financial guidance, including advice for their employer, training for employer's staff (as necessary);
- ensure the Customer is aware of any changes to their benefit entitlement and ensure that they are receiving all appropriate in work benefits by sign-posting them to JCP for expert advice;
- if appropriate, ensure the Customer is aware of their rights as a disabled person (as defined by the Equality Act 2010);
- liaise with the Access to Work Specialist Advisory Team, where appropriate, to provide advice and support about accessibility solutions; and
- conduct individual exit planning in the final stages of the Programme.

In addition, for Customers in the Intense Service Strand, the Service Provider must provide:

- Job Analysis and Task Analysis. Customers will be offered In-Work Support specific to their particular needs. Job Analysis must be undertaken for each Customer entering employment to inform the In-Work Support Action Plan, which, with Customer consent, must be agreed with the employer. For Customers who have been supported through the Supported Employment Framework this will also include a description of the job coaching they are receiving and a plan for withdrawing this support over time; and
- those following the Supported Employment Framework can also expect job-coaching, reducing over time as appropriate

Within this Specification, the Scottish Government has provided detailed service requirements both at a Service level and in relation to the 3 Service Strands of Core/Advanced/Intense.

12. Partnership, Integration and Alignment

12.1 The approach to delivery set out in this Specification will require the Service Provider to build and maintain excellent working relationships with key stakeholder organisations and groups to help provide effective and joined up support for Customers. These include but will not be limited to:

- The Scottish Government;
- Customer Representative Groups;

- Jobcentre Plus;
- Local Authorities;
- Skills Development Scotland;
- Third Sector Employability and Specialist Service Organisations;
- Centres for Independent Living;
- Integration Joint Boards (Health and Social Care);
- Employers (in the public, private and third sectors);
- Social Service Teams and Organisations;
- Carer Groups;
- Organisations that represent the interests of disabled people with a disability (e.g. user groups);
- Education and Learning Institutions;
- NHS e.g. Mental Health Support Teams;
- Healthy Working Lives Centres;
- Alcohol & Drug Partnerships;
- Organisations that represent the interests of people with convictions; and
- Organisations working in Homelessness.

12.2 The Scottish Government has a long standing ambition for greater integration and alignment across public sector delivery. Devolution of employment services provides an opportunity to not only build on the strengths of existing national and local services but to develop a long-term plan that will set out the Scottish Government's vision for achieving greater alignment and integration.

12.3 Building on existing good practice, effective engagement with such partners (at an appropriate level) will help to ensure that services recognise and reflect local needs, priorities, strategies and resources to achieve best outputs and value for money, and offer a comprehensive service that meets the needs of all Customers.

12.4 The Service Provider is required to take into account local initiatives and publically funded services to support an agenda to improve performance and the quality of support to individuals, reduce duplication of spending by public sector bodies and improve the effectiveness of the use of public funds in the locality in which services are being provided.

12.5 The Service Provider is required to work closely with such partners and accept working with such partners is a service requirement.

12.6 As part of on-going quarterly Contract reviews, the Service Provider is required to discuss their efforts to encourage partnership, integration and alignment. This extends to the sharing of good practice, challenges and risks across the Lot.

12.7 In addition, the Service Provider is required to participate in 6 monthly Scottish Government led employment services 'share and learn' events at a national level, to share best practice, data, what works, etc.

13. Employer Engagement

13.1 To achieve high levels of good quality job outcomes, employer engagement will be key to the success of the Service. The Scottish Government will actively work with the Service Provider and other stakeholder/partners to ensure high quality employer engagement which addresses:

- the need for the Service Provider to have a strong understanding of existing and emerging labour markets across the Lot;

- the need wherever possible to align with local and national employer engagement strategies or plans to avoid duplication;

- the development of mutually beneficial relationships with employers which enable the Service Provider to influence employers positively in terms of the staff they recruit on the basis of business benefits that can be accrued; and

- links to existing Scottish Government policies, including the Scottish Business Pledge, Fair Work ambitions, and efforts to tackle inequality and occupational segregation.

13.2 Scottish Government expects the Service Provider to engage with employers by demonstrating that the Service is designed to better meet their recruitment needs by including substantial employer involvement, which offers Customers:

- first-hand information relating to the world of work;

- the opportunity to discuss 'what makes a successful employee' with employers;

- the opportunity to undertake job interview practice with a local employer;

- awareness of 'first impressions' – dress to impress and personal hygiene;

- visits to local employer premises;

- short work experience opportunities; and

- the opportunity for Customers to discuss issues with existing employees.

14. Stakeholder Engagement Strategy

14.1 The Service Provider must develop, deliver and maintain a Stakeholder Engagement Strategy ("the Strategy") to reflect how the Partnership, Integration and Alignment and Employer Engagement requirements will be met.

14.2 The Strategy must be supported by a detailed Stakeholder Engagement Plan which outlines the Service Provider's approach to engaging, working effectively and collaboratively with the external stakeholders to maximise Customer outcomes.

14.3 The Scottish Government will require Service Providers to refine their Stakeholder Engagement Plan with the Scottish Government prior to the Service Delivery 'Go live' date of the contract and progress will be monitored at the monthly Contract Performance Reviews.

14.4 The Stakeholder Engagement Plan must clearly describe how the Service Provider will achieve greater integration with existing local services and health provisions and must include as a minimum: the interventions, timelines/ frequency of engagement, delivery methods of engagements and communications with the broad range of local stakeholders and support services.

14.5 The Stakeholder Engagement Plan must explicitly detail how the Service Provider will engage and work with employers to a) allow employers to feed into the Service design and delivery b) support and encourage employers to employ Customers using the Service.

14.6 As part of on-going quarterly Contract Performance Reviews, the Service Provider is required to discuss their efforts to encourage partnership, integration and alignment. This will extend to the sharing of good practice, challenges and risks across their Lot.

14.7 The Service Provider will be required to provide an updated Stakeholder Engagement Plan every three months. The Stakeholder Engagement Plan and any amendments to it will be subject to the approval of the Scottish Government.

15. Service Provider Behaviours

15.1 In line with the Scottish Government's principles and values, where the Service Provider sub-contracts, enters into partnership agreements or forms consortia for the Service delivery, they must:

- be committed to achieving the best possible outcomes for its Customers;
- act with integrity in their dealings with these parties;
- ensure transparency, non-discrimination, equal treatment and clearly defined accountability in relationships between parties;
- encourage the sharing of good practice;
- agree, document and abide by the terms of delivery and funding at the outset;
- agree monitoring and management information requirements that are not overly bureaucratic and must be consistent, proportionate, clearly specified and agreed at the Effective Date;
- develop and support its sub-contractors or partners to improve overall supply chain effectiveness;
- agree and deliver a level of support for all parties; in particular any new entrants into the market; and
- be transparent about decisions or referrals of Customers to delivery partners including the level and type of support needed.

16. Branding, Communications, Marketing and Accessibility

16.1 While the Scottish Government will actively market the Service prior to the service start date, the Service Provider- is also required to pro-actively market and promote the Service, reaching out and engaging Customers who may not have previously accessed available employment support once the Service has commenced.

16.2 Given the voluntary nature of the service, the Service Provider must develop innovative and effective communications and marketing activities to attract Customers and enthuse them to engage and attend on a regular basis.

16.3 The Service Provider will be required to use the agreed Scottish Government Branding for the Service (which is owned by the Scottish Government). The Branding will be provided to the Service Provider on the Effective Date.

16.4 The Service Provider shall ensure that the Fair Start Scotland name and branding is included on all communications (including promotion and marketing material) relating to the delivery of the Service.

16.5 The Service Provider must ensure that dedicated feedback inbox details are given to Customer and promoted/displayed on marketing leaflets and public areas of Service Provider's premises.

16.6 The Service Provider must note that the following domain names belong to the Scottish Government:

- fairstartscotland.co.uk
- fairstart.org.uk

- fairstartscotland.org.uk
- fairstartscotland.uk
- fairstartscotland.com
- fairstartscotland.org
- fairstart.scot
- fairstartscotland.scot

16.7 The process and guidelines for use of the Scottish Government Logo and Fair Start Scotland Logo are detailed in the Operational Guidance.

16.8 All communications (press releases, announcements, advertising, publicity material or activity and similar such communications) associated with the operation of the Service must be submitted to the Scottish Government for approval. The Service Provider must not issue any communications until written/email confirmation is received from the Scottish Government confirming that the communication is approved and can be issued.

16.9 The Service and all its content, notices, templates, forms, marketing material and associated services must be provided in English. If required, the Service Provider must make documentation available in other languages, in audio format, in Braille, large print and in other formats.

16.10 Access to portals and associated documentation must be comprehensive, clearly laid out and be easily understood by all users.

16.11 All Customer user guides must be assessable to users with visual or other disabilities and be compatible with industry-standard screen readers or other assistive technology (compliant to Level AA of the Web Content Accessibility Guidelines (WCAG) / ISO 40500:2012 or equivalent).

17. Feedback, Suggestions, Complaints and Escalation

17.1 The Service Provider must operate a quality feedback process for Customers, ensuring the voice of the Customer is recognised and valued in service delivery and demonstrates how this shapes provision going forward, ensuring systems are in place to encourage Customers to feedback on their experience of the Service. This must include suggestions for improvement; positive feedback and complaints.

17.2 For complaints, the Service Provider must put in place an internal dispute resolution procedure to deal with issues raised by Customers regarding the delivery of this Service. This must include clear and reasonable timescales as detailed below for resolution and a defined escalation process. The Service Provider must acknowledge receipt of complaint/concern within 2 working days of receipt and provide a formal response to Customer within 5 working days of receipt (copied to the Scottish Government for information).

17.3 If the dispute between the Customer and the Service Provider (and/or the Sub-Contractor) cannot be resolved the dispute shall be referred to the Scottish Government, who will independently review the dispute and make a final determination within 10 working days.

17.4 The Service Provider will provide a dedicated feedback e-mail address as part the Induction process. This must be supplemented by a non-digital solution for Customers unable to access email.

17.5 The Induction Pack, issued by the Service Provider to its Customers, must also advise that the feedback be copied to a dedicated Scottish Government inbox. This will allow the Scottish Government to effectively monitor feedback without placing an undue burden on the Service Provider. This feedback will be considered and emerging themes or concerns discussed as a part of contract performance reviews. The Induction Pack needs to be clear that responsibility

for dealing with feedback and in particular complaints is initially the responsibility of the Service Provider.

17.6 The Service Provider must ensure that its complaints process includes provision for allegations of serious misconduct.

17.7 The main types of serious misconduct include, but are not limited to:

- racial abuse;
- sexual abuse;
- serious breach of professional conduct;
- theft or fraud; and
- criminal activities.

17.8 The Service Provider must inform the Scottish Government immediately upon receipt of a complaint in this category. The Service Provider must also consider suspending any (employee or) sub-contractor from continuing delivery until any investigations into the complaint has been completed.

17.9 The Service Provider must liaise with the Scottish Government on the outcome of any investigation into a serious complaint. If a serious complaint is upheld, the Service Provider must consider liaising with the relevant professional body and request revocation of approval from the Scottish Government.

17.10 The Service Provider shall report monthly to the Scottish Government on the number and nature of complaints received, source of the complaint, and the average time taken to resolve complaints as detailed within Schedule 1.

18. IT

18.1 The Scottish Government intend to introduce an IT system to support delivery of Fair Start Scotland during the life of the contract. The Scottish Government will work with the Service Provider to develop and introduce a new digitally enabled system developed around the needs of service users.

19.2. In the event that the IT solution is not fully available before Service commencement in April 2018, the Scottish Government will provide a contingency option which may include:

- a hybrid clerical and electronic system.

19.3. The contingency will support referrals to the Service using widely available desktop technologies.

19.4. Scottish Government will provide assistance to the Service Provider in utilising a hybrid clerical and electronic system and will ensure that proper Change Control procedures (see Schedule 3) will be implemented.

19.5. The Service Provider must note that the Scottish Government will not provide an electronic service to manage the Service Provider's relationship with Customers, i.e. a case management solution. The Service provider will undertake their own case management function and put in place their own case management solution.

19. Innovation

19.1 The Scottish Government is committed to a programme of innovation work that will aim to drive greater integration and alignment between employment support and other key services, such as health, justice and skills, during the lifetime of the contract, to improve outcomes for participants and explore how the commissioning of employment services can support this approach.

19.2 Doing so will require an approach on learning and innovation that:

- Encourages, or at the very least does not inhibit, delivery-led innovation by devolved Service Providers;
- Encourages other public services, partners and devolved Service Providers to work together so devolved support services can lead on and participate in new and innovative practices; and
- Creates the space for testing new ideas, taking risks, learning and sharing.

19.3 The Scottish Government is exploring the development of an Innovation Fund alongside the 2018 Service as one way of delivering this approach. The Service Provider may be asked to be involved in the development or delivery of innovation work, subject to further discussion with the Scottish Government.

20. Performance Requirements

20.1 The Scottish Government 2015 consultation document highlighted that any employment programme should pursue sustainable employment as its key outcome and measure of success.

20.2 The Scottish Government has provided clarity on expectations on Customers (both who they are and how many there should be), service requirements and performance expectations, while at the same time leaving scope for Service Providers to draw on their intelligence and experience to secure a robust and ambitious set of contracts which are the foundation for a successful service.

20.3 However, operating an entirely voluntary programme on this scale represents a departure from comparable employment support programmes in the UK over the last 10-20 years, which have been underpinned by degrees of mandatory engagement and systems within which the commissioner has considerable control over both the supply and demand sides of the service.

20.4 Some of these fundamental elements are absent in the devolved Scottish context and this will require a more responsive and partnership focussed relationship between the Scottish Government and the Service Provider to address these challenges collectively.

20.5 Policy development in respect of tackling inequality and Fair Work at Scottish Government level mean that income levels and the need to try to address in-work poverty, aligned to aspirations of a Scottish Living Wage for all – have an increasing importance.

20.6 In addition to the outcome measure set out below, the Service Provider shall measure the extent to which Customers are moving into Scottish Living Wage jobs (and in which sectors) and will work with the Scottish Government to agree how this is gathered.

20.7 For the reasons set out above, the Scottish Government has an aspiration to measure job outcomes through income using the HMRC Real Time Earnings (RTE) data currently available to DWP. Prior to reaching agreement with HMRC, Job Outcomes will be defined as a minimum of 16 hours per week worked at the National Minimum Wage (NMW) or above, appropriate to their age over either a continuous or cumulative period of employment.

20.8 The Service Provider is required to provide evidence to verify the number of hours worked each week by each Customer (and shall obtain a disclaimer from the Customer to allow the Service Provider to contact the employer to verify employment and earnings). As part of the validation process, the Scottish Government will conduct checks on a sample basis to ensure they meet all requirements (see Schedule 2: (Contract Charges, Payments and Pricing)) (and this activity shall also be covered by the disclaimer obtained by the Service Provider).

20.9 For research and evaluation purposes, any available data on actual earnings that can be collected pending agreement with HMRC should be recorded and stored by the Service Provider.

20.10 The performance expectations for Customers are outlined below and represent a minimum level of performance from the Referral Period on each Service Strand and at a Programme level. Details on how the performance expectations have been established are attached at Annex D, (Customer Volumes and Contract Values) of this Schedule.

20.11 Minimum Performance Expectations in respect of the Key Performance Indicators at a Strand Level:

Service Strand	13 week Job Outcomes (% of starts on the Programme)	26 weeks Sustained Job Outcome (% of 13 week Job Outcomes)	52 weeks Sustained Job Outcome (% of 13 week Job Outcomes)
Core Strand	41%	84%	70%
Advanced Strand	27%	84%	70%
Intense Strand	28%	84%	70%

20.12 The above Minimum Performance Expectations are based on the following assumptions of how those starting the Programme will attach to each service strand:

- 14% of Customers will be supported through the Core Service Strand.
- 50% of Customers will be supported through the Advanced Service Strand.
- 36% of Customers will be supported through the Intense Service Strand.

20.13 The Service Provider's performance will be measured on a cohort performance metric. This metric is derived from the following information:

- The number of starts per Service Strand each calendar month;
- The minimum performance level for each Service Strand;
- The profile or distribution for the length of time between Customers being referred to the Service and achieving a job outcome; and
- A one month lag has been added between a job outcome being achieved and a job outcome being claimed to allow for administrative activities.

20.14 Further detail on cohort performance metrics are contained within the operational guidance.

21. Outcomes not eligible as Job Outcomes

21.1 In defining the types of opportunity which may be considered a job outcome and will therefore not count towards the Service Provider meeting the KPIs:

- Community Jobs Scotland training opportunities; and
- any job which has been created through the provision of a wage subsidy. The Scottish Government insist on a drive towards real jobs.

22. Management Information

22.1 In addition to management information gathered from the Scottish Government supporting IT systems, the Service Provider shall provide routine management information reports to the Scottish Government.

22.2 The Service Provider shall provide management information reports or data exchange in electronic and computer readable formats. The format (or online) will use CSV, XML, Word, Excel or other format as appropriate to the purpose of the data. The format, content and transport mechanism of the required management information will be agreed between the Scottish Government and Service Provider. The content and data of the reports will belong to the Scottish Government, and the Scottish Government will define the Data specification standards that the Service Provider will need to comply to.

22.3 Reports are to be provided to the Scottish Government on a monthly basis, no later than 10 working days following the end of each month during the Contract Period. Reports or data extracts may include, but not be limited to, the following information which must be collected and available for reporting as required:

If applicable i.e. Customer does not start on the Service after referral to Service Provider:

- Reason for failure to attend
- Reason for failure to start

Customer information (to be gathered at start of Programme):

- Date of Birth
- Gender*
- Ethnic Group*
- Long-term health condition/ disability*
- Sexual Orientation*
- Religion*
- Gender reassignment*

*Scottish Government will provide advice on the questions to be asked, and the mode of collection to be used

- Name
- Address, including full postcode
- Benefit in receipt of
- NI number
- Contact details and preferred method of contact
- ESOL support needs
- Literacy or Numeracy support needs
- Length of unemployment
- Reason for leaving last job.

*Scottish Government will provide advice on the questions to be asked, and the mode of collection to be used

Referral criteria – whether the Customer is:

- Someone with convictions (someone who has completed a custodial sentence or a community sentence) or offender (someone who is completing a custodial or community sentence)
- Care experienced
- A lone parent
- A refugee
- From an ethnic minority
- A health condition which presents a barrier to employment
- Living in one of the 15% most deprived SIMD areas
- Long term unemployed (2 years+)
- Disabled (as defined in the Equality Act 2010)

On-Programme information

- Programme referrals
- Programme starts
- Job starts:

    - Employer details
    - Contract type
    - Contract hours

- Job Outcome (3 months)
- Job sustainment (6 months)
- Job sustainment (12 months)
- All information relating to and recorded as part of the Customer Action Plan.
- Wider (softer) Customer outcomes -'distance travelled' towards work

Job outcome achieved: (3 months)

- Found permanent employment
- Self employed
- Living/ Scottish Living wage job
- Employment sector

Job sustainment (6 months)

- With same employer as 3 month outcome
- With 1 or more different employers

Job sustainment (12 months)

- With same employer as 3 month outcome
- With same employer as 6 month outcome
- With 1 or more different employers

Other positive destination achieved

- Entered other forms of training
- Progression or return to College
- Progression or return to University

Reasons for leaving Programme without an outcome prior to completion

- Customer does not wish to continue participating (disengages)
- Personal issues prohibiting participation (not health-related)
- Health related issues
- Financial issues
- Relocated / Moved Away
- Serious Injury
- Pregnancy
- Death
- Detained in custody
- Education or training
- Other (please specify)

Provider-based information

- Client/advisor ratios;
- The use of wage subsidies (including Intermediate Labour Market) and their impact on performance;
- Details of any particular areas where there are specific delivery challenges, including but not exclusively rural. Any relevant case studies would be helpful;
- Current levels of co-ordination/integration with other services, how this is used and how well it is working. This will inform priorities for future integration;
- Good news stories;
- Case studies;
- Details of Community Benefits being delivered.

22.4 In addition to the monthly management information report, the Service Provider shall produce an Annual Report in May of each year, and a final overarching Report at the end of the Contract.

22.5 The overarching Annual Report must contain both narrative and statistical data based on aggregated management information up to and including the period of the annual report, along with a broader narrative on the added value and impacts of the Service to both the Service Provider and wider/ local partners.

22.6 The Scottish Government will use the management information to produce statistics, include in published information documents or any such associated requirement to use the information.

23. Performance Management

23.1 The Service Provider shall monitor and report on performance against the Service Levels and the Contract.

23.2 The Key Performance Indicators and Key Delivery Indicators are detailed at Annex E and F of this Schedule. These requirements will be measured as part of the overall performance of the Service Provider, utilising individual Customer case management notes to evidence progress and outcomes.

23.3 The Service Provider's performance against the Service Levels will be checked by the Scottish Government's Performance Management and Operational Support Team on a monthly basis. The Service Provider must provide the Scottish Government with its full cooperation in this process and will be required to provide full access to its systems and evidence as required to conduct the checks at such times as the Scottish government may require.

23.4 The Scottish Government will assess the Service Provider's performance using such means or methods as it considers appropriate in the circumstances (which may include (without limitation) a strategic performance management tool to assess quality, service, delivery and cost).

23.5 The Scottish Government will utilise monthly performance and management information available from the supporting IT or clerical systems, for performance management purposes, and the Service Provider must provide additional monthly/ ad-hoc management information (as set out in Management Information within paragraph 23 of this Schedule) within 10 Working Days following the end of each month.

23.6 The Scottish Government has the right to request information and access to records in relation to Programme delivery at any time and the Service Provider will provide any and all such information which is requested. Response times for this type of ad-hoc request will be determined by the Scottish Government on a case by case basis at the time of the request, however the Service Provider must note that on occasions, such as receipt of a Request for Information, the Scottish Government's requests will require a prompt response and in any case within such time as the Scottish Government may determine at the time of making the request.

23.7 The Service Provider will be responsible for all costs associated with the provision of management information. Annex E (Performance Expectations) to this Schedule contains the Key Performance Indicators and key delivery Indicators designed to measure delivery, service, quality and cost in relation to the Contract. Any additional Service Levels will be agreed prior to the Commencement Date.

23.8 The Service Provider will be responsible for ensuring delivery of the Services in accordance with the Service Guarantee for the Contract Period.

23.9 Any additional specific Service Levels will be agreed using the procedures set out in Schedule 3 (Change Control Procedures).

23.10 The Service Levels may need to be revised/added to over time and the Service Provider shall continuously improve and reset the Service Levels to increase performance, where appropriate as reasonably requested by the Scottish Government and agreed in accordance with Schedule 3 (Change Control Procedures).

23.11 Duly authorised staff or agents of the Scottish Government shall have the right to visit sites used by the Service Provider to deliver the Service and to be given access to the Service Provider's records and staff (and/or those of its sub-contractor) and to Customers during the hours when the Service Provider is delivering the service with a view to verifying that the Service Provider is delivering the Service in accordance with the Contract.

24. Tracking Period

24.1. Where the Customer leaves the Programme without the Service Provider meeting any of the Outcomes in respect of such Customer, then:

24.1.1. where the Service Provider is able to evidence that the Customer has commenced employment within the 6 weeks immediately following the relevant Customer leaving the Programme (such 6 week period known as the **"Tracking Period"**); and

24.1.2. where such employment started by the relevant Customer during such Tracking Period meets the Outcomes then the Service Provider shall be allowed to claim for the relevant Outcome payments in respect of such Customers.

24.2 Where the Customer leaves the Programme the tracking period lasts for 6 weeks, and will commence on the date a Customer leaves their period of pre-Employment Support without a job.

24.3 This six week period allows the Service Provider to claim Job Outcome payments for Customers who move into employment (that meets the Job outcome definition stated in paragraph 29.11) within six weeks of formally leaving Fair Start Scotland.

25. Monitoring and Evaluation Activities

25.1 The Scottish Government may require additional information from the Service Provider in order to monitor and evaluate the success of provision and their management and delivery of the Services. The Service Provider must co-operate fully with any monitoring and/or evaluation activity commissioned by the Scottish Government. This may include provision of details of Customers' age, gender, ethnicity, disability, progress and achievements.

25.2 Evaluation will seek to investigate the extent to which the Service meets its aims, objectives, Key Performance Indicators, Key Delivery Indicators and process measures. The Service Provider must participate fully in the evaluation and share key learning to help inform the Scottish Government's future service delivery plans. This will include, but not necessarily be limited to, participating in interviews with the Service Provider to learn from their perspectives, assisting in the generation of a sampling frame of Customers from whom interviewees will be selected and providing relevant management information when required. The Service Provider will be required to support the Scottish Government in seeking Customer Consent to use and share data, and to facilitate Customers joining an Experience Panel on attachment to the Programme.

25.3 The Scottish Government is likely to externally commission elements of the evaluation and the Service Provider may be asked to provide information directly to the appointed third parties. The aim of the evaluation is to provide a holistic picture of impacts at an individual, group and system level. For example, elements of the evaluation are likely to include:

i) process measures – to gather feedback from Customers, providers and other stakeholders on factors affecting the delivery of services;

ii) assessment of hard outcomes, using a number of routes where possible, including using Service Providers' management information and through direct surveying of individuals. The Scottish Government is investigating the possibility of linking with data from HMRC on jobs/earnings: and

iii) exploration of softer outcomes - using a mix of methods (e.g. questionnaires, interviews and focus groups) to measure individual and group level impacts such as Customer satisfaction, self-confidence and perceived health benefits.

25.4 The Scottish Government will wish to be able to break findings down to show impacts, for example, for the three Service Strands, at different Lots and for different groups (e.g. age, sex, ethnicity, disability etc.) where possible.

25.5 The management information collected, performance assessment undertaken and annual reports will provide an important contribution to the information needs of the evaluation strategy. The management information requirements are shown at paragraph 23 of this Schedule.

26. Assurance and Fraud Team Reviews

26.1 The Assurance and Fraud Team's primary role is to provide the Scottish Government with an assurance that:

- Payments for employability support services are in accordance with the Scottish Government and Treasury requirements;
- Public funds and Scottish Government data are protected; and
- Value for money has been obtained.

26.2 The Assurance and Fraud Team will review the Service Provider's internal control systems to assess their ability to manage risk across three key areas:

- **Governance Arrangements** – to ensure the Service Provider has robust governance arrangements, systems for tracking and reporting performance and anti-fraud measures;
- **Service Delivery** – to ensure the Service Provider has effective systems for administering the Customer Journey to ensure that Scottish Government is receiving the service it is paying for. The review will also include the management of the supply chain;
- **Financial Procedures** – to ensure the Service Provider has effective systems in place to support their claims for payment, including appropriate segregation of duties.

26.3 The Scottish Government expects the Service Provider to proactively self-assess their management and delivery of the Service. The Assurance and Fraud Team will review the Service Provider's self-assessment activities as part of the assurance process.

26.4 Further about the Assurance and Fraud Team role and the Provider Assurance requirements are detailed in the Terms and Conditions and the Operational Guidance.

27. Continuous Improvement

27.1 The Service Provider will actively seek to improve performance through a policy of Continuous Improvement designed to deliver Service efficiencies, reductions in whole-life costs and improvements in quality and performance throughout the Contract Period.

27.2 The Service Provider's Continuous Improvement Strategy will focus on delivering Service efficiencies and improvements in quality, performance and opportunities for better integration and alignment of services. The Service Provider will maintain a record of Continuous Improvement initiatives and their outcomes.

28. Service Budget and Funding Model

28.1 The Service will be wholly funded by the Scottish Government. The Service will be provided free of charge to all eligible Customers.

28.2 The charges for the Service are detailed within Schedule 2 (Pricing).

28.3 The Scottish Government's 2015 consultation on devolved services highlighted the need for sufficient guaranteed funding to enable smaller organisations to engage and guarantee a level of support for all Customers.

28.4 Therefore the funding model for this Service is intended to reflect the cost of supporting the needs of the Customers in the three Service Strands as outlined in the Customer journeys.

28.5 The Scottish Government will put in place a service fee and payment by results based funding model which is consistent in proportion across all Customer groups.

28.6 The funding model will consist of:

- Implementation Costs;
- Service fee;
- Job outcome fee paid at 13 weeks sustainability; and
- Further Sustained Job Outcome Fees at 26 and 52 weeks of sustained employment.

28.7 The Service Fee is based on 30% of the total contract value (excluding implementation costs) from the Service Providers bid. This will be paid in monthly instalments irrespective of the volumes starting the Programme, as set out in Schedule 2 (Pricing).

28.8 **Job Outcome payments** where a Customer has entered a job and sustained for 13 weeks, 26 weeks and 52 weeks. The proportion of total outcome fees will be set at:

- Job Outcome fee at 13 weeks: 15%
- Sustained Job Outcome fee at 26 weeks: 35%
- Sustained Job Outcome fee at 52 weeks: 50%

28.9 The Service Provider will be able to claim payment for sustained job outcomes following 13, 26 & 52 weeks of employment based on Customer being in work for a cumulative period of 13 weeks in a 16 week period, 26 weeks in a 30 week period and 52 weeks in a 60 week period.

28.10 The Service Provider will be able to claim payment for job outcomes achieved within the 'Profiling and Planning Activities' period (Weeks 1-8) based on the Core Service Strand rate as outlined in Schedule 2 (Pricing).

29. Payment Validation Process

29.1 The Scottish Government will validate outcome payments on a regular basis by conducting a series of pre and post payment checks. Further information about the validation process and the evidence requirements are detailed in Schedule 2, Annex A (Pricing).

30. Key Delivery Indicators - Validation Process

30.1 The Service Provider is required to maintain a robust system of internal control that needs to be sufficient not only to support achievement of Key Delivery Indicators (KDI) but also to allow internal management checks to be undertaken and independent testing and validation, by Scottish Government. The records maintained should document how and when the KDIs were achieved and any appropriate supporting evidence was obtained.

30.2 The Scottish Government does not prescribe the way in which the Service Provider should track Customers or record information about their activity. However, these must be capable.

30.3 The Service Provider remains accountable for making sure that all KDI outcomes are checked.

30.4 KDIs which fail validation or the Scottish Government is unable to validate will be subject to a challenge period. This provides the Service Provider with the opportunity to seek review by submitting additional information which allows the Scottish Government to reconsider.

30.5 Each month the Scottish Government will randomly select for validation a sample of Customer records. Please note, the Scottish Government reserve the right to sample additional records at any point. The Service Provider will be informed by Scottish Government on who has been selected within the sample.

30.6 The sample will be subject to checks to establish if KDIs relevant to the sample have been met.

30.7 Where one or more KDIs have not been met, and following the challenge period, the Service Credit process described at Schedule 2 (Pricing) shall apply.

31. Customer Travel Expenses

31.1 Customers must not be financially disadvantaged due to their attendance at the Service. However, some Customers may **already** receive support for such costs due to a health condition; therefore they must not be over-compensated.

31.2 The Service Provider is responsible for reimbursement of all appropriate travel costs and any additional support costs incurred. The Service Provider must not assume that the Customer is entitled to travel costs, and must ensure appropriate checks are made before payment is made to the Customer, and that the most appropriate mode of transport has been utilised by the Customer depending upon their level of health condition, disability or any other barrier to travel.

31.3 Where the Customers travel costs are to be paid or reimbursed, these costs must not exceed Scottish Government standard travel rates (i.e. those that are currently applicable at the point of costs being incurred by the Customer) which are provided within Schedule 2 (Pricing).

31.4 Data on Customer costs must be provided in accordance with the provision of management information and to meet audit and governance requirements. This will include the submission of receipts and/or vouchers.

32. Childcare Costs

32.1 Customers will be entitled to childcare costs if this is a barrier to attending the Service. The Service must be delivered, where possible, within the hours to suit the Customer, but where this cannot be met, or no alternative funding sources can be identified, childcare costs may be considered.

32.2 The Service Provider is responsible for arranging to provide childcare costs associated with the Customer's attendance on the Service. These will be paid in agreement with Scottish Government at standard rates and reclaimed on an agreed basis.

32.3 Data on Customer costs must be provided in accordance with the provision of management information and to meet audit and governance requirements. This will include the submission of receipts and/or vouchers.

32.4 Further information on agreement of Childcare Costs and the rate of payment will be provided in the Operational Guidance.

33. Additional Costs

33.1 The Service Provider is responsible for payment of any additional costs incurred where a Customer needs extra help to attend and participate fully in the Service. This may include grants, clothing, specialist equipment that is required to support the Customer take up an employment opportunity. Appropriate checks must be made before agreeing to provide the funding requirement, including exploring alternative funding options.

33.2 Data on Customer costs must be provided in accordance with the provision of management information. This will include the submission of receipts or vouchers where appropriate.

33.3 DWP guidance on Access to Work will be updated to reflect devolved employment services. The Service Provider must take note of the guidance in relation to expenses covered by Access to Work and those covered by providers in contracted support for those in work.

34. Open Book Accounting

34.1 Open Book Accounting ("**OBA**") will provide the Scottish Government with information that will be invaluable in helping to understand all costs associated with the Service delivery and help to inform future funding models and Service delivery and design. This includes:

- understanding expenditure (cost base);
- understanding the cost implications of decisions taken or being considered in delivering the Service and forward investment;
- operating and managing the Service to incentivise and drive improvements in cost efficiency;
- how Service Providers and their sub-contractors can work together to develop and implement a proactive approach to Service decision making and create a positive experience for the Customer; and
- help the Scottish Government understand the cost drivers in delivering this service, learn about the prime/sub v consortium delivery approaches and the scope for future efficiencies.

34.2 The Information that the Service Provider will share with the Scottish Government will include, but not be limited to, the following:

- Data on actual Service Provider and sub-contractor costs, margins, trends and volumes. Likely to include both actual and forecast data;
- Information on process, systems and quality controls put in place to manage and ensure compliance;
- Any other financial or non-financial data gathered continuously or periodically that supports innovation, Continuous Improvement or decision making.

34.3 Specific OBA requests from the Scottish Government will be discussed with the Service Provider on a case by case basis.

35. Contract Management and Key Contract Milestones Dates

35.1 The key contracting dates are detailed below. These provide an overview of the Contract timelines, milestones and the final invoicing date which is fully detailed in Schedule 2 (Pricing).

Activity	**Date(s)**
Contract Award	1st November 2017
Implementation and Mobilisation	2nd November 2017 to 31 March 2018
Operational Service Commencement Date (i.e. First Customer Referral)	13 March 2018
Service Delivery Go Live Commencement Date (i.e. Customer Start)	3 April 2018
Last Customer Referral:	2 April 2021
Last Pre-employment Support	1 April 2022

Note: In exceptional cases Pre-employment Support may be extended for up to 6 months for Customers in the Intense Strand. The last date for Customers on Pre-employment Support is:	30 September 2022
Last date for In-work Support (i.e. Contract expiry date). Note: This date applies only to Customers assigned to the Intense Service Strand whose pre-employment period was extended by 6 months.	24 November 2023

36. **Contract Extension**

36.1 The Scottish Government, subject to satisfactory Service Provider performance, the continuing need for the service and availability of budget will reserve the option to extend the contract for up to two years as contained in Clause 4.2 of the Contract.

37. Contract Management

37.1 The Scottish Government considers the effective performance and delivery of the Services to be a business critical objective of the Contract. As such, the Service Provider shall be open, flexible and transparent in the operation, management and delivery of the Contract and shall develop and implement appropriate due-diligence, risk management and quality assurance measures to ensure that Services are delivered on time, within budget and in accordance with the Service Levels.

37.2 The Service Provider must provide and maintain adequate management and staff resources, including a Service Manager to support the strategic and day to day operation and management of the contract.

37.3 The Service Manager shall hold a senior position and have sufficient influence with the Service Provider's organisation to be able to promptly respond on the Service Provider's behalf to the Scottish Government's requests, queries and complaints.

37.4 The Service Manager shall act as the single point of contact for the purposes of operating the Contract and will be responsible for the effective mobilisation, implementation, delivery and exit management of the Contract.

37.5 The Service Manager shall ensure that the Service Levels are achieved and consistently high standards of service and best practice are assured and maintained throughout the duration of the Contract.

37.6 The Service Provider must ensure that all staff engaged in the performance of the Contract have and maintain an appropriate level of knowledge and expertise; are appropriately trained and qualified; and are competent to deliver the required Services. This may include, but is not limited to: training on the tasks to be performed; operation of the Contract; and procedures concerning health and safety at work, data protection and sustainability.

37.7 The Service Provider must ensure that there is a sufficient level of trained and competent staff to operate and manage the Contract at all times and that an adequate reserve of trained staff and competent staff are available during holidays, sickness and/or any other absence.

38. Contract Review Meetings

38.1 The Service Manager shall be required to attend monthly Governance and Review meetings with the Scottish Government.

38.2 The Service Manager may also be required to attend additional ad-hoc meetings at times and locations specified by the Scottish Government, including the quarterly meetings referred to in paragraph 13, Partnership, Integration and Alignment.

38.3 The Governance and Review Meetings will address operational issues such as Service delivery and achievement of the Service performance requirements.

38.4 The Scottish Government may on occasion request that specific sub-contractors attend the monthly meetings if this is deemed to be necessary.

38.5 All costs incurred by the Service Provider in attending review meetings will be the responsibility of the Service Provider.

39. Change Control Procedures

39.1 In addition to the service requirements within this Specification, the Service Provider shall embrace changes (proposed by the Scottish Government) to the delivery model to reflect emerging good practice; or adapt to changes to policy to ensure the delivery of the principles and values outlined in this document. Any such requirements will be subject to formal discussions and agreement according to the change control procedures detailed at Schedule 3 (Change Control Procedures).

40. Mobilisation and Implementation

40.1 During the implementation period, the Service Provider shall provide the Services in accordance with the Implementation Plan to ensure the Services will be fully functional in order that: i) the Operational Services will be ready to commence on the Services Commencement Date; and ii) the Go Live Services will be ready to commence on the Services Go-Live Commencement Date.

40.2 The Service Provider will be responsible for managing the successful mobilisation and implementation of the Contract in accordance with the Implementation Plan and shall provide sufficient resources to ensure the availability and provision of the Services in accordance with the Contract from the Service “Commencement Date”.

40.3 The Service Provider must submit a detailed Implementation Plan to the Scottish Government for approval no later than 10 Working Days from the **Effective Date (the “Detailed Implementation Plan”)**. The Service Provider shall not be entitled to propose any variations to the Scottish Government milestone dates set out in the Initial Implementation Plan.

40.4 The Scottish Government shall review and comment upon the Implementation Plan as soon as reasonably practicable and in any case, no later than 10 Working Days from its receipt. Following such review and consultation, the Scottish Government shall formally approve or reject the Implementation Plan.

40.5 If the Scottish Government rejects the Detailed Implementation Plan, it shall provide its reasons for the rejection and the Service Provider shall have the period of 10 Working Days from the date of the rejection in which to revise and re-submit the Implementation Plan for approval. The parties shall use all reasonable endeavours to resolve any disputes and agree the Detailed Implementation Plan as soon as possible. If the parties are unable to resolve any disputes this shall be referred to the Management Arrangements (Schedule 4).

40.6 The Service Provider will update the Detailed Implementation Plan on a monthly basis (or as otherwise directed by the Scottish Government) until such time as all Milestones have been Achieved and shall submit the updated plan to the Scottish Government's Contract Manager within 10 Working Days prior to the end of each month. The provisions of clauses 40.3 and 40.4 shall apply mutatis mutandis provided that the references to 10 Working days shall be reduced to 5 Working Days.

40.7 The Service Provider will appoint a named Service Manager to manage the mobilisation and implementation of the Contract. The Service Manager will act as the Single Point of Contact (SPoC) for the Scottish Government. The Service Provider will also specify a named contact to the Scottish Government for the escalation and progression of any issues associated with the mobilisation and implementation process.

41. Data Management

41.1 The Service Provider shall ensure that all information held or obtained by the Service Provider in connection with the operation of the Contract is securely and sensitively managed at all times and in accordance with Schedule 9 (Model Contract regarding Data Protection Directive 95/94/EC).

42. Exit Strategy

42.1 The Service Provider shall develop and maintain plans and procedures for the orderly transition of the Services to a successor Service Provider in accordance with Schedule 10 (Exit Management).

43. Business Continuity & Disaster Recovery

43.1 The Service Provider shall have in place and maintain appropriate and relevant Business Continuity and Disaster Recovery plans, policies and procedures in respect of the Services in accordance with Schedule 11 (Business Continuity and Disaster Recovery (BCDR)).

44. Physical Data Security

44.1 The Service Provider shall ensure robust and layered physical security measures are in place at all sites where data is stored. This must include, but not be limited to:

- limited access to server room (authorised personnel only);
- low key appearance;
- limited entry points to server room;
- door control system, including Fire Doors.

Penetration Testing

44.2 The Service Provider must confirm that associated IT systems are tested on an annual basis by an accredited tester and that vulnerabilities are actioned in line with recommended actions.

44.3 The Scottish Government further require that an accredited penetration test specific to the hosted website(s) be conducted annually, or earlier should significant changes be implemented that have the possibility of introducing weaknesses to those systems. Recommended actions should be implemented to remove or mitigate any discovered vulnerabilities. This will ensure that checks are aligned with business objectives (i.e. scope, constraints, deliverables) and that remedial actions are actioned in line with business requirements.

44.4 The Service Provider shall develop and maintain an Information Security Management System and Security Management Plan within the provisions of Schedule 12 (Security).

45. Storage of Data

45.1 The Service Provider must store all data relevant to this Contract (whether personal data or otherwise) in a secure data storage environment which must be located within the European Economic Area.

45.2 This data must be stored in a manner that allows authorised persons to easily access and retrieve data.

46. Risk

46.1 The Service Provider shall, at all times, have in place an appropriate risk management strategy (including a suitable risk management plan and risk logs) for the delivery and support of Services to be provided under the Contract.

46.2 The Service Provider must inform the Scottish Government immediately of any known or foreseeable risks which may have an impact on the operation of the Contract and/or the performance of the Services.

47. Sustainability, Environmental and Community Benefits

47.1 The Service Provider shall comply with the Scottish Government's sustainable development strategy and ethical policy with respect to the delivery of this Contract.

47.2 The Service Provider's policies and processes will support the Scottish Government's 'Greener Scotland' strategic objective including: a proactive approach to sustainable consumption and the efficient use of resources; consideration given to social and environmental consequences; policies which ensure that business activities have a direct positive impact on climate change and energy; and policies which encourage natural resource protection and environmental enhancement.

47.3 The Scottish Government is committed to sustainable procurement and to this end the Service Provider is required to comply with all social and environmental policies in the delivery of Services during the period of the Contract.

47.4 The Service Provider will be required to report to the Scottish Government within their monthly management information reporting, details of any sustainability and environmental measures and achievements.

47.5 'Community Benefits' are social considerations which include not only targeted recruitment & training, but also equal opportunities, training for the existing workforce, supply-chain initiatives, community consultation, 'considerate Supplier' schemes, contributions to education, the promotion of social enterprises and resources for community initiatives.

47.6 The Service Provider shall embrace the Scottish Government's requirement for delivering Community Benefits through the Contract. To assist the Scottish Government in understanding what opportunities exist to deliver benefits to the community through the Contract, the Service Provider shall report to the Scottish Government as part of their monthly management information reporting, details of any Community Benefit measures and achievements such as Targeted Recruitment and Training, skills development, employment, apprenticeships, etc.

47.7 The Public Sector in Scotland is committed to the delivery of high quality public services, and recognises that this is critically dependent on a workforce that is well rewarded, well-motivated, well-led, has access to appropriate opportunities for training and skills development, are diverse and is engaged in decision making. These factors are also important for workforce recruitment and retention, and thus continuity of service. Public Bodies in Scotland are adopting Fair Work practices, which include:

- a fair and equal pay policy that includes a commitment to supporting the Living Wage, including, for example being a Living Wage Accredited Employer;

- clear managerial responsibility to nurture talent and help individuals fulfil their potential, including for example, a strong commitment to Modern Apprenticeships and the development of Scotland's young workforce;

- promoting equality of opportunity and developing a workforce which reflects the population of Scotland in terms of characteristics such as age, gender, religion or belief, race, sexual orientation and disability;

- support for learning and development;

- stability of employment and hours of work, and avoiding exploitative employment practices, including for example no inappropriate use of zero hours contracts;

- flexible working (including for example practices such as flexi-time and career breaks) and support for family friendly working and wider work life balance; and

- support progressive workforce engagement, for example Trade Union recognition and representation where possible, otherwise alternative arrangements to give staff an effective voice.

47.8 In order to ensure the highest standards of service quality in this Contract, the Service Provider shall take a similarly positive approach to Fair Work practices as part of a fair and equitable employment and reward package.

Annexes to the Specification and Service Levels

Annex A to Schedule 1: Sources of Information

1. Creating a Fairer Scotland: A New Future for Employability Support in Scotland: http://www.gov.scot/Resource/0049/00498123.pdf

2. Creating a Fairer Scotland: Employability Support: http://www.gov.scot/Resource/0048/00481121.pdf

3. ONS, Labour Force Survey, Apr-Jun datasets, 2016 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/workingandworklesshouseholds/aprtojune2016

4. The Scottish Government Disability Delivery Plan http://www.gov.scot/Publications/2016/12/3778

5. ONS Labour Force Survey, June-August 2016 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/uklabourmarket/october2016

6. Equalities Act 2010 http://www.legislation.gov.uk/ukpga/2010/15/introduction

7. *Scottish Index of Multiple Deprivation (SIMD)*[7] http://www.gov.scot/Topics/Statistics/SIMD

8. Employability Pipeline http://www.employabilityinscotland.com/employability-pipeline/

9. EU How to Guides on Supported Employment http://www.euse.org/index.php/resources/how-to-guides

10. The Scottish Living Wage http://scottishlivingwage.org/

11. Supported Employment Framework for Scotland http://www.gov.scot/Resource/Doc/303629/0095168.pdf

12. The Scottish Government http://www.gov.scot/Home

13. The Scottish Business Pledge https://scottishbusinesspledge.scot/

14. The Scottish Government's Diversity and Equality Policy http://www.gov.scot/Topics/People/Equality

15. The Scottish Government's Labour Market Strategy (including Fair Work Agenda) http://www.gov.scot/Publications/2016/08/2505

Annex B to Schedule 1: Service Guarantee

All Customers will be entitled to a service guarantee, as summarised below:

Initial Engagement (Day 1)

- Initial contact within 5 working days of referral to arrange first interview.
- A face to face initial assessment within 10 working days of referral to confirm eligibility and an action plan for the Discovery and Planning phase (see below) of the Programme.
- Allocation to a named key worker who will be your adviser for the duration of the Programme
- Agreement of a Participation Agreement, setting out the commitments of each party.
- **Intense Service Strand Only:** Speedy referral to specialist providers for Customers assessed as needing support through the Intense Service Strand.

Discovery and Planning Phase (1 to 8 weeks)

- Weekly interventions with key worker
- Face to face monthly review with key worker;
- Baseline assessment of employability skills;
- Better Off in Work calculation and financial planning; and
- Planning for additional support to be provided by external or partner services;

- **Core and Advanced Service Strands Only:** Development of a detailed personalised Employment Action Plan which sets out agreed activities and timescales to help you into work including activities for overcoming barriers including engagement with external services, current skills, employment history, vocational training needs, employment aspirations, monitoring and review arrangements and in-work support plan.

- **Intense Service Strand Only:** Vocational Profiling leading to an individual action plan

Pre Work Support (9 to 52 weeks)

- Minimum of 3 hours weekly contact with key worker;
- 1 to 1 coaching by key worker as necessary;
- Face to face formal monthly review with key worker;
- Quarterly distance travelled assessment and feedback;
- Employability activities as detailed in the individual Employment Action Plan;
- Engagement with external or partner services as detailed in the individual Employment Action Plan;
- Monthly workplace reviews (if on work placement);
- Weekly job search activities;
- Employer engagement including support for interviews and negotiations of reasonable adjustments; and
- Financial guidance.

- **Intense Service Strand Only:** Support to overcome recruitment barriers;
- **Intense Service Strand Only:** Job matching with suitable vacancies, including job carving; and
- **Intense Service Strand Only:** Job carving during work experience placements (if necessary)

In-Work support (Job entry date + 52 weeks)

- An In-Work Support Action Plan, detailing timeline for workplace reviews with employer, future training and career development goals and actions;
- Minimum of weekly contact with key worker, fading as appropriate;
- Minimum monthly workplace review with employer, reducing over time as appropriate
- Workplace induction; Support at workplace training (if necessary);
- Support to develop workplace relationships;
- Financial guidance; Advice for employer, training for employer's staff (as necessary); and
- Individual exit planning in the final stages of the Programme

- **Intense Service Strand Only:** Job Analysis;
- **Intense Service Strand Only:** Task Analysis (if necessary); and
- **Intense Service Strand Only:** Workplace job coaching, reducing over time as appropriate

Annex C to Schedule 1: Lots

Lot	Local Authorities Areas	% share of potential Customers *
Glasgow	Glasgow	**20.0%**
Lanarkshire	North Lanarkshire South Lanarkshire	**13.2%**
Tayside	Angus Dundee City Perth and Kinross	**7.6%**
Forth Valley	Clackmannanshire Falkirk Stirling	**5.2%**
East	City of Edinburgh East Lothian Fife Midlothian Scottish Borders West Lothian	**22.2%**
Southwest	East Ayrshire Dumfries and Galloway North Ayrshire South Ayrshire	**10.5%**
North East	Aberdeen City Aberdeenshire	**5.9%**
Highlands and Islands	Argyll and Bute Eilean Siar Highland Moray Orkney Islands Shetland Islands	**6.4%**
West	East Renfrewshire Inverclyde Renfrewshire East Dunbartonshire West Dunbartonshire	**9.0%**

* References to Lot 'West' in this Specification are for information purposes only. Lot West is for Supported Businesses.

Annex D to Schedule 1: Customer Volumes & Contract Values

Assumption on the number of individuals attaching to each service strand

Until the Scottish Government Segmentation Tool has been finalised and tested, the Scottish Government has built assumptions, at a national level, on the extent to which each of our Customer groups will be supported within the Core, Advanced and Intense Service Strands. These assumptions were provided to inform Service Providers in developing their proposals for the each Lot(s).

Service level	Eligible Groups	Take Up	Total	% of Starters
Core	JSA 24+			**14%**
	Early Entry			
	Total Eligible Population		12,700	
	Initial Take Up	*60%*	7,620	
	Final Take Up	*70%*	**5,334**	
Advanced	JSA 24+			**50%**
	ESA WRAG			
	Early Entry			
	Total Eligible Population		45,100	
	Initial Take Up	*60%*	27,060	
	Final Take Up	*70%*	**18,942**	
Intense	ESA WRAG			**36%**
	Early Entry			
	Total Eligible Population		18,390	
	Initial Take Up	*60%*	11,034	
	Final Take Up	*70%*	7,724	
	ESA Support		1,500	
	Non-Claimants		4,500	
	Total		**13,724**	
	Total Attachments		**38,000**	

The above percentages have been used by the Scottish Government to determine the minimum performance expectations detailed in this Annex.

Recognising the entirely voluntary nature of the Programme, the Scottish Government has built in assumptions on how the eligible population relates to programmes starts based on available comparable evidence of both voluntary and mandatory programmes in Scotland and the UK:

- The Scottish Government has assumed an initial take up rate of 60% in each service strand which articulates the extent to which we expect the eligible population to volunteer and be referred to the Programme, this is described as the initial take up rate;

- The Scottish Government has also assumed that 70% of those voluntary referrals will actually start on the Programme, this is described as the final take up rate.

The above assumptions have been used by the Scottish Government to determine the minimum volume/performance expectations detailed in this Annex. In addition, the Scottish Government has included a drop-out rate of 10% against all Service Levels, again reflecting the entirely voluntary nature of the Programme, on those who start the Programme.

Calculation of the Minimum Performance Expectation

The Scottish Government has established Minimum Performance Expectations (MPE) at the 13 week Job Outcome point on each service level. Analysis was conducted to determine which client groups are most likely to be supported in each service level and a performance baseline for each strand was created by assessing the performance of comparable client groups over the duration of the Work Programme in Scotland.

The Scottish Government then tested this Work Programme baseline against key differences in the 2018 Scottish service, including its voluntary nature, to identify performance uplift within the 2018 programme. When added to the Work Programme baseline, this creates the MPE for the service.

Service Level	Scottish Government Client Groups	Work Programme Groups	WP Performance	SG Performance Uplift	Minimum Performance Expectation
Core	JSA 24+ Early Entry	JSA 25 and over JSA Early Entrants	30%	11%	41%
Advanced	JSA 24+ ESA WRAG Early Entry	JSA 25 and over New ESA claimants: Excluding 12 Month prognosis claimants JSA Prison Leavers	17%	10%	27%
Intensive	ESA WRAG ESA Support Early Entry Non-Claimants	New ESA claimants: Excluding 12 Month prognosis claimants New ESA claimants: 12 Month prognosis claimants only JSA Prison Leavers ESA Ex-Incapacity Benefit	14%	14%	28%

Sustainment of performance at the 26 and 52 weeks points is consistent across all service levels and is based on comparable data on UK and Scottish Contracted Employment Support programmes.

LOT split based on contract value and the minimum volume expectations

The table below sets out the Lots shares based on the percentage benefit claimant share and minimum programme starts (38,000).

The data has been calculated by assessing the total population of JSA, ESA and UC benefit claimants in Scotland and calculating each Lot's percentage share of this total.

Lots	Glasgow	Lanarkshire	Tayside	Forth Valley	East	Southwest	Northeast	Highlands and Islands
Local Authorities	Glasgow	North Lanarkshire South Lanarkshire	Angus Dundee City Perth and Kinross	Clackmannanshire Falkirk Stirling	City of Edinburgh East Lothian Fife Midlothian Scottish Borders West Lothian	Dumfries & Galloway East Ayrshire North Ayrshire South Ayrshire	Aberdeen City Aberdeenshire	Argyll and Bute Eilean Siar Highlands Moray Orkney Islands Shetland Islands
% Benefit Claimant Share	20%	13.2%	7.6%	5.2%	22.2%	10.5%	5.9%	6.4%
Estimated Contract Value (£)	19,100,000	12,600,000	7,300,000	5,000,000	21,300,000	10,100,000	5,600,000	6,200,000
Estimated Starts	7,600	5,000	2,900	2,000	8,400	4,100	2,200	2,400

Note. The table above excludes information for Lot: 'West' which is reserved for Supported Businesses.

LOT Split on Minimum Performance Expectations

Lot: Glasgow								
Strand	**Assumed Starts %**	**Assumed Starts**	**13 Week Job Outcome %**	**13 Week Job Outcome**	**26 Week Sustain % of 13 Week JO**	**26 week Sustain**	**52 week sustain % of 13 week JO**	**52 week sustain**
Core	14%	1064	41%	436	84%	366	70%	305
Advanced	50%	3800	27%	1026	84%	862	70%	718
Intense	36%	2736	28%	766	84%	644	70%	536
Total	**100%**	**7600**	**29%**	**2228**	**84%**	**1872**	**70%**	**1560**
Total	**100%**	**2900**	**29%**	**850**	**84%**	**714**	**70%**	**595**
Advanced	50%	4200	27%	1134	84%	953	70%	794
Intense	36%	3024	28%	847	84%	711	70%	593
Total	**Total**	**8400**	**29%**	**2463**	**84%**	**2069**	**70%**	**1724**

Annex E to Schedule 1: Key Performance Indicators

Ref.	Key Performance Indicator	Measurement
1.	**Job Outcomes:** Must be for a minimum of 16 hours per week paid at NMW which has lasted 13 weeks in a 16 week period. For self-employment the Customer must have traded independently, working at least 16 hours per week for their business for 13 weeks at NMW; provided the job meets the outcome criteria you will be entitled to claim for a job outcome. This will be confirmed by the individual.	The Service Provider's performance in respect of this Outcome shall be reviewed and measured monthly by the Scottish Government using performance data to ensure the Service Provider's monthly projections on performance have been achieved. Paragraphs 21.13, 21.14 and 25 if this Schedule shall apply
2.	**Sustained Job Outcomes (26 weeks)':** Must be for a minimum of 16 hours per week paid at NMW. Employment must have lasted 26 weeks out of 30 weeks. For self-employment the Customer must trade independently working at least 16 hours per week for their business for 26 weeks at NMW, from date of employment outcome. This will be confirmed by the individual. (Breaks in employment must total no more than 4 weeks).	The Service Provider's performance in respect of this Outcome shall be reviewed and measured monthly by the Scottish Government using performance data to ensure the Service Provider's monthly projections on performance have been achieved. Paragraphs 21.13, 21.14 and 25 if this Schedule shall apply
3	**Sustained Job Outcomes (52 weeks):** Must be for a minimum of 16 hours per week paid at NMW. Employment must have lasted 52 weeks out of 60 weeks. For self-employment the Customer must have traded independently, working at least 16 hours per week for 52 weeks out of 60 week period at NMW, from date of employment. This will be confirmed by the individual. (Breaks in employment must total no more than 8 weeks).	The Service Provider's performance in respect of this Outcome shall be reviewed and measured monthly by the Scottish Government using performance data to ensure the Service Provider's monthly projections on performance have been achieved. Paragraphs 21.13, 21.14 and 25 if this Schedule shall apply
	*Note: Any period of self-employment can only be counted once regardless of whether the participant has one or multiple self-employed occupations during that period.	

Annex F to Schedule 1: Key Delivery Indicators

All Strands

Ref.	Key Delivery Indicators	Measurement	Service Level
1	**Start Date and Service Induction (Stages 4 and 5)**. Start/Induction Interview to be completed face to face within 5 Working Days from receipt of the referral.	Measured monthly via a random Sample of Service Providers' caseload management records	90%
2	**Start Date and Service Induction (Stages 4 and 5)**. For any Customer whose Start/Induction interview is not completed within the 5 Working Days timeline as outlined in Ref.1 above, the Start/Induction Interview must be completed within 10 Working Day from receipt of the referral.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
3	**Start Date and Service Induction (Stages 4 and 5)**. Service Provider must immediately notify the Customer and Referral Agency in writing of the date and time of their Start Date/Induction Interview after the warm handover process detailed in Stage 3.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
4	**Start Date and Service Induction (Stages 4 and 5)**. 48 hours prior to the Start Date/Induction Interview a courtesy telephone call to be made by the Service Provider to the Customer to alleviate any Customer's concerns.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
5	**Start Date and Service Induction (Stages 4 and 5)**. At the Induction Interview, the Service Provider must provide each Customer with an Induction Pack.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
6	**Intervention / Customer Engagement (All Stages)** At every weekly face to face intervention, a	Measured monthly via a random Sample of Service Providers' caseload management records	100%

Ref.	Key Delivery Indicators	Measurement	Service Level
	Customer's personalised Action Plan will be reviewed and updated to reflect progress and agreement of future activities and actions.		
7	**Intervention / Customer Engagement (All Stages)** Face to face formal monthly review between the Key Worker and the Customer to take place.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
8	**Segmentation Tool** Segmentation Tool must be completed by Customer prior to start on the Programme.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
9	**Segmentation Tool** Service strand to be confirmed by end of week 3 commencing from the referral of the relevant Customer.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
10	**In Work Support Plan (Stage 10)** A detailed In Work Support (IWS) Plan to be agreed with the Customer within 10 Working Days of job start.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
11	**Procedure for Disengagement by Customer** The Service Provider must contact the Customer within 1 Working Day to establish circumstances surrounding disengagement from being notified by the Customer that they will not continue with the Programme.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
12	**Procedure for Disengagement by Customer** If the Service Provider is unable to engage the Customer within 5 Working Days of either i) failing to attend service provision they must contact the Referral Agency or ii) failing to establish circumstances surrounding disengagement as outlined in 11 above.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
13	**Customer Programme Exit and Leaver Plan (Stages 8 and 9)**. The Service Provider must produce a detailed Leavers Plan for each Customer returning to the Referral Agency, within 10 Working Days of Customer's end date.	Measured monthly via a random Sample of Service Providers' caseload management records	100%

Ref.	Key Delivery Indicators	Measurement	Service Level
14	**Complaints**. The Service Provider must acknowledge receipt of complaints/concerns within 2 Working Days of receipt.	Measured monthly by the Scottish Government via a random sample of Service Providers' caseload management records.	100%
15	**Complaints**. Service Provider must provide a formal response to Customer within 5 Working Days (copied to the Scottish Government) of the complaint being raised.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
16	**Specialist Support** Service Provider must facilitate immediate referrals and access to specialist support to address health problems, including professional help to manage mental/physical health conditions and well-being interventions.	Measured monthly via a random Sample of Service Providers' caseload management records	100%

Annex F to Schedule 1: Key Delivery Indicators - Intense Strand Only

Ref.	Key Delivery Indicator	Measurement	Service Level
17	**In Work Support Plan (Stage 10)** Job Analysis must be undertaken for each Customer entering employment to inform the In-Work Support Action Plan, which, with Customer consent, must be agreed with the employer.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
18	**Vocational Profiling** All Customers must be offered Vocational Profiling.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
19	**Supported Employment Model and Individual Placement and Support** The Supported Employment Model for disabled people and Individual Placement and Support (IPS) must be available and offered.	Measured monthly via a random Sample of Service Providers' caseload management records	100%

Key Delivery Indicators: Performance Reporting

Ref.	Delivery Indicator	Measurement	Service Level
20	**Management Information** The Service Provider is required to provide management information to the Scottish Government in accordance with this Specification	Accurate monthly management information must be provided within 10 Working Days of the end of each month.	100%
21	**Stakeholder Engagement Plan** The Service Provider is required to provide an updated Stakeholder Engagement Plan every 3 months commencing from the **"Commencement Date"** and report progress of partnership, integration and alignment activities with local organisations and services.	Measurements and milestones to be agreed post contract award.	100%

Annex G to Schedule 1: Integration and Alignment with Other Scottish Government Services

The Scottish Government has set out a programme of public sector reform which includes an ambition for much greater integration of services. A list of current Scottish Government funded Services is set out below, with an indication of its purpose and how it will align or integrate with the new employment programme.

There must be no expectation that these initiatives will run for the duration of Fair Start Scotland contract.

Service	**Integration and Alignment**
Opportunities for All – an offer of training or education for young people not in education employment or training.	The new service is part of the integrated offer of support.
Activity Agreements	The new service will be part of the support young people on Activity Agreements will be able to access from age 18 if it is appropriate for them.
Community Jobs Scotland	Service Providers may believe this service suitable and appropriate for their Customers, in which case and on the assumption that eligibility conditions are met and a suitable opportunity is available, they can do so. However, this will not be considered a job outcome for the purposes of the contract pricing model.
SERI	SERI is a wage subsidy for new jobs including apprenticeships. Service Providers may believe this suitable and appropriate for their Customers, in which case and on the assumption that eligibility conditions are met and a suitable opportunity is available, they can do so. However, this will not be considered a job outcome for the purposes of the contract pricing model.
Open Doors In Work Support 16-29	This is specialist in-work support. The Scottish Government expect high quality in-work support as part of the new service. Access to this for service Customers would be duplication of funded support, so will not be possible.
Modern Apprenticeships	Articulation from employment services to Modern Apprenticeships is a key ambition. Access to Modern Apprenticeships will be defined as a job outcome. The apprenticeship must be expected to last 12 months or more.
Employability Fund	The Employability Fund will remain a key part of the pre-contracted support provision for DWP Customers and will align with devolved services at this time. Service Providers must make provision for short sharp skills interventions available to Customers in line with Customer need and opportunities in the local labour market.
Individual Learning Accounts	Participants on the new service cannot access ILAs.

Annex H to Schedule 1: Additional information on Supported Businesses

The Scottish Government is committed to furthering the development of supported businesses in Scotland. We have set up the Supported Business Advisory Group (SBAG), the Framework for Supported Factories and Businesses; actively promoting the use of Regulation 21 of the Public Contracts (Scotland) 2015 Regulations within public sector procurement and commissioning the 2013 independent Review of Supported Businesses in Scotland. SBAG is chaired by the Minister for Business, Innovation and Energy.

One of the aims of SBAG is to increase the amount of public contracts placed with Supported Businesses. Scottish Government is represented on SBAG and is expected to be an exemplar by increasing the amount of contracting activity with Supported Businesses by considering sustainability as part of the award criteria for regulated procurements and where possible the use of Regulation 21 of the Public Contracts (Scotland) 2015 Regulations.

A Supported Business is defined in the Public Contracts (Scotland) Regulations 2015 as:

> **"an economic operator whose main aim is the social and professional integration of disabled or disadvantaged persons and where at least 30% of the employees of the economic operator are disabled or disadvantaged persons;"**

Annex I to Schedule 1: Technical Response Document

Technical Response is provided under separate WORD document

Annex J to Schedule 1: Clarifications

Clarifications are provided under separated WORD document

This and the following 11 pages comprise Schedule 2 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 2 - PRICING SCHEDULE

1. The Purchaser will pay the Service Provider the Contract Charges as outlined in Annex 2 to this Schedule for the provision of the Services in accordance with the Specification and Service Levels (Schedule 1) and the rest of the Contract.

2. All Outcome payments shall be FIXED (i.e. not subject to change) in respect of Customer referrals received during the Initial Referral Period as outlined in clause 4.1.1 of the Contract (Period) and any increase to the Outcome payments following the Initial Renewal Period shall be determined solely in accordance with paragraph 3 of this Schedule..

2.1 All Service fees shall be fixed (i.e. not subject to change) for the period commencing from the Services Commencement Date until the end of the Initial Referral Period and any increase to the Service fees following the Initial Referral Period shall be determined solely in accordance with paragraph 3 of this Schedule.

3. Indexation

3.1. Should the option to extend the Contract be taken up, at the sole discretion of the Purchaser, based upon clause 4.2 of the Contract (Period), the Contract Charges for such extended period shall be negotiated between the Parties and such negotiated price shall not exceed the Contract Charges derived using the following methodology:

3.2. Indexation will be applied to the Outcome payments in accordance with the annualised Consumer Price Index ("CPI"), as provided by the Office for National Statistics, for the December in the Purchaser's financial year immediately preceding the commencement date of the relevant Contract extension. Any such increase shall be applied once per extension on the commencement date of the relevant Contract extension and the indexed rates will be applicable over the entire duration of the relevant extension. For example, the Outcome payments for 2021-22 would be uplifted by 2.5% if annualised CPI for December 2020 was 2.5%. These indexed fixed fees would be applicable over the 1 year extension period.

3.3 Indexation will be applied to one year's Service fees (being the total Service fees as shown in Annex 2 to this Schedule divided by four (4)) in accordance with the annualised Consumer Price Index ("CPI"), as provided by the Office for National Statistics, for the December in the Purchaser's financial year immediately preceding the commencement date of the relevant Contract extension. Any such increase shall be applied once per extension on the commencement date of the relevant Contract extension and the indexed rates will be applicable over the entire duration of the relevant extension. For example, the Service fees for 2021-22 would be uplifted by 2.5% if annualised CPI for December 2020 was 2.5%. These indexed fixed fees would be applicable over the 1 year extension period.

4. Not Used

5. Supporting Information related to Pricing

The funding approach has the following payment elements and ratios:

5.1. Implementation Costs

5.1.1 The Purchaser recognises that some costs will be incurred prior to the Services Commencement Date. Implementation costs can be paid as a part of the Contract if the Service

Provider considers this beneficial. Where Implementation costs are paid, these shall be outlined in Annex 2 to this Schedule.

5.1.2. Where the Service Provider wishes to be paid for these costs separately they will be fixed and on a cost recovery basis only. These costs shall be paid in arrears at such times as outlined in Annex 2 to this Schedule and subject to the retention outlined in paragraph 5.2.3 of this Schedule and always after they have been incurred by the Service Provider. No mark up or Service Provider profit margin in relation to these costs will be accepted. Additionally, only those costs which need to be met by the Service Provider prior to the Services Commencement Date will be considered for payment by the Purchaser. For example, where the cost relates to staff salaries, only payments incurred by the Service Provider in respect of any period in which they are employed on the implementation of the Programme as outlined in the Contract up to the Services Commencement Date will be considered for payment.

5.1.3. Where the Implementation costs are paid under the Contract, the Purchaser shall withhold 30% of the total Implementation costs until the Service Provider commences to provide all the Go Live Services. The Purchaser shall release the retained Implementation costs where the Service Provider is ready to provide the Go Live Services even where no Customers have been referred to the Service Provider, provided that this is not due to a Default of the Service Provider.

5.2. Service Fee

5.2.1. The service fee will equate to 30% of the total Contract price (excluding any implementation and contingency costs agreed). The service fee is intended to provide a degree of certainty in meeting fixed costs associated with delivery of the Service and will be paid monthly in arrears. The service fee shall be payable over three years from the Services Commencement Date in respect of the period from the Services Commencement Date until the end of the Initial Referral Period.

5.2.2. The service fee will then be further divided into Year 1; Year 2; and Year 3 Service Fees based on 50% (Year 1); 30% (Year 2); and 20% (Year 3) of the initial 30% of the total Contract price. These amounts will then be further divided into equal monthly payments for each year.

Example:

(Note: the overall cost is not intended to represent actual costs)

Overall Costs for Service (excluding Implementation)	£ 100,000
Total Service Fee	£ 30,000 (£ 100,000 x 30%)
Year 1 Service Fee	£ 15,000 (£ 30,000 x 50%)
Monthly Service Fee	£ 1,250 (£ 15,000 / 12 months
Year 2 Service Fee	£ 9,000 (£ 30,000 x 30%)
Monthly Service Fee	£ 750 (£ 9,000 / 12 months)
Year 3 Service Fee	£ 6,000 (£ 30,000 x 20%)
Monthly Service Fee	£ 500 (£ 6,000 / 12 months)

5.3. Outcome Payments

5.3.1. The overall amount available for Outcome payments will equate to 70% of the total Contract price (excluding any implementation and contingency costs agreed).

5.3.2 The Service Provider shall render an invoice on a monthly basis in respect of all the Outcomes achieved during the previous month in respect of Customers. The Service Provider shall provide to the Purchaser any and all evidence the Purchaser may request to support such invoice.

5.4. Achievement of Job Outcomes

5.4.1. Job Outcomes payments will be made on a unit price basis, which will be calculated by dividing 15% of the Outcome payments described above by the number of Job Outcomes as outlined in Annex 2 to this Schedule. These payments will only be made in respect of Customers to whom Key Performance Indicator 1 applies, as outlined in Annex E to the Specification.

5.5. Achievement of First Sustainment Payments

5.5.1. First Sustainment Payments will be made on a unit price basis, which will be calculated by dividing 35% of the Outcome payments described above by the number of first sustainment Outcomes as outlined in Annex 2 to this Schedule . These payments will only be made in respect of Customers to whom Key Performance Indicator 2 applies, as outlined in Annex E to the Specification.

5.6. Achievement of Second Sustainment Payments

5.6.1. Second Sustainment Payments will be made on a unit price basis, which will be calculated by dividing 50% of the Outcome payments described above by the number of second sustainment Outcomes outlined in Annex 2 to this Schedule . These payments will only be made in respect of Customers to whom Key Performance Indicator 3 applies, as outlined in Annex E to the Specification.

5.7 Contingency Costs

As detailed in Section 19 of the Specification, the IT solution for managing referrals and outcome payments is still under development. THE Service Provider's contingency costs for a hybrid clerical and electronic system are outlined in Annex 2 to this Schedule.

5.8 Payment validation

The provisions of Annex 1 to this Schedule 2 shall apply to all payments by the Purchaser to the Service Provider. No payment in respect of paragraph 5.4 shall be due unless the Service Provider's claim for payment has been validated in accordance with the procedures outlined in Annex 1 to this Schedule 2

6. Service Credits

6.1. The Service Credits shall be calculated with reference to any of the below events occurring for an individual Customer who engages with the Programme. For the avoidance of doubt this includes pre start employability activities through to their end of In-Work Support activities. The number of events which have occurred shall be multiplied with the Service Credit value allocated to each event.

6.2. The Service Credit value shall be calculated using the Service Provider's service fee as set out below:

- The service fee for each service strand shall be divided by the number of Customers anticipated in each strand as outlined in Annex D of Schedule 1 to calculate a notional service fee per Customer per strand ("Notional Service Fee").

6.3. The Service Credit value in respect of Key Delivery Indicators 1-16, as detailed within Annex F to Schedule 1, shall be equivalent to one sixteenth of the Notional Service Fee for each occasion where the Service Provider fails to meet the specified service level for the relevant Key Delivery Indicator.

6.4. For the Intense Strand only, the Key Delivery Indicators 17-19 the Service Credit value shall be equivalent to the entire Notional Service Fee for that strand for each occasion where the Service Provider fails to meet the specified Service Level for the relevant Key Delivery Indicator.

Service Credits	Service Credit Value
Failure to meet Key Delivery Indicators 1-16	£ per Key Delivery Indicator failure
Failure to meet Key Delivery Indicators 17-19	£ per Key Delivery Indicator failure

6.5. Where relevant, following identification of an event occurring, the Purchaser shall render an invoice in respect of the amount to be recovered as detailed in the methodology for calculation of Service Credits outlined in this Schedule. Such invoice shall be payable by the Service Provider to the Purchase no later than 30 days from the date of invoice.

Payment Validation Process

1.1. The Service Provider must have robust financial and accounting procedures in place to meet audit requirements. These must include details of all financial transactions and supporting evidence in relation to all payments. The Service Provider shall provide assistance to the Purchaser for the Purchaser to be able to complete the validation process as the Purchaser may require.

1.2. The Service Provider shall only submit accurate claims for payments that they are entitled to under the Contract. The Purchaser will utilise its own systems to satisfy itself that the claims are valid. This will include a series of checks to confirm that Customers have started and remained in employment or self-employment for the required period of time and have worked the hours and fulfil any other requirements as outlined in the Contract.

1.3. The Service Provider is required to maintain a robust system of internal control that not only supports any claims for payment but also allows internal management checks to be undertaken and independent testing and validation, by the Purchaser and other external bodies. The records maintained shall document how and when the appropriate supporting evidence was obtained.

1.4. Where a Customer has not given consent to contact employers, this must be recorded by the Service Provider. In these cases the Purchaser will only contact the Customer. Where consent has been given, the Purchaser will contact the relevant employer and/or the Customer in an attempt to validate the claim.

1.5. The Service Provider shall track Customers and record information about their employment activity. There is however specific information in relation to each Customer that the Service Provider is required to document and submit to the Purchaser when it submits claims for payment in respect of an Outcome:

- Whether the period is employment or self-employment
- Employer/s contact details including address, contact name, full business telephone number and email address
- The Customer's contact details
- Start date of employment/self-employment
- End date of employment/self-employment (if applicable)
- The number of hours worked in each week
- Confirmation that the Customer is earning National Minimum Wage (NMW) as a minimum
- The working/shift pattern

1.6. The Service Provider remains accountable for making sure that all Outcomes are checked prior to making a claim for payment and that all such claims must be valid at the point of submission for payment.

1.7. The Service Provider shall promptly notify the Purchaser where it becomes aware of any information in respect of claims for payment and/or payments (prior to sampling in accordance with paragraphs 1.9 and 1.20) which require a claim to be withdrawn to allow the Purchaser to arrange for the recovery of funding where the fee has been paid and to allow the claim to be removed from the system.

1.8. Claims which fail validation or which the Purchaser is unable to validate will be subject to a challenge period. This provides the Service Provider with the opportunity to seek review by submitting additional information which allows the Purchaser to have another attempt at validation.

1.9. Each month the Purchaser will randomly select for validation a sample of claims which have been paid by the Purchaser (the size of the sample to be determined by the Purchaser) in the previous month. If the total of claims paid is less than the specified sample in any month then all claims will be selected. The Purchaser reserves the right to sample additional claims at any

point in its sole discretion. The Service Provider will be informed by the Purchaser of the Customers who have been selected within the sample.

1.10. The sample of Job Outcome claims will be subject to checks to establish if Customers have been in work, for at least 16 hours per week, for 13 weeks out of 16 weeks (from the job start date), paid at NMW with no breaks in employment (or, in the case of a self-employed Customer, they have traded independently for at least 13 weeks) as outlined more specifically in the KPIs.

1.11. The Purchaser may in the future decide to measure Outcomes through income using the HMRC Real Time Earnings (RTE) data currently available to DWP.

1.12. The Service Provider can meet the KPI even if the Customer's employment is made up of more than one employer as long as 16 or more hours are completed and paid at NMW in each week. Where the Purchaser identifies that the other conditions for the KPI have not been met in respect of the Customer's employment or self-employment, then the claim will fail validation.

1.13. Where the Purchaser identifies during validation that the job start date is prior to the date the Customer started on the Programme, the claim will fail validation, unless the Customer has increased hours to a minimum of 16 hours per week paid at the NMW, as outlined more specifically in the Key Performance Indicators in Annex E to the Specification.

1.14. Where the Purchaser establishes that a Customer has not been in work for a sufficient time at the point when the claim is submitted to the Purchaser to meet the requirement but at the point of validation the Customer meets all requirements as outlined in the relevant Key Performance Indicators, the claim will be treated as a Technical Pass.

1.15. Where a Customer has not given consent to contact employers the Purchaser will only attempt validation via the Customer. Where the employer is unable/ unwilling to validate the claim, the Purchaser will contact the Customer. In cases where the Purchaser is experiencing difficulty making contact with the employer and/or the Customer, the Purchaser may, but is not obliged to, contact the Service Provider to confirm the details the Service Provider has supplied. For example, where the Purchaser believes that the Service Provider has submitted incorrect or incomplete information (e.g. unobtainable telephone numbers).

1.16. The Service Provider is required to establish the correct information and supply it promptly to the Purchaser to maximise the chances of positive contact. If the Service Provider does not provide the detail that enables the Purchaser to complete validation, the claim will fail validation.

1.17. Error rates are derived from checking a representative sample of claims and extrapolating against the remaining population of claims. This means the correct level of payment and performance will be attributed to a Service Provider. Therefore the Purchaser will not accept a request to withdraw a claim once a sample has been drawn.

1.18. There are four possible validation results:

- **"Pass"** – An employer and/or Customer confirms the condition for payment has been met, as set out in the Outcome

- **"Technical Pass"** – at the manual validation stage there are two scenarios:

    - An employer/Customer confirms that there is a valid claim however the details provided by the employer and/or Customer and the details supplied by the Service Provider differ. The Purchaser will inform the Service Provider of the correct information and the Service Provider will update its records. The payment will not be recovered and will not contribute to the error rate for extrapolation.

    - If the Purchaser establishes that a Customer has not been in work for a sufficient time within the claim period to meet the requirement but at the

point of validation they have (and meet all requirements), the claim will be treated as a Technical Pass. The payment will not be recovered and will not contribute to the error rate for extrapolation.

- **"Fail"** – An employer/Customer provides information which means the condition for payment, as set out in the KPIs, has not been met. The claim is recorded as an error and will contribute to the error rate for extrapolation.

- **"Unable to Validate"** – the Purchaser has either not been able to contact the employer and/or Customer, or the employer and/or Customer are unable/ unwilling to provide the information required to validate the claim.

1.19. Unable to Validate claims will be apportioned across the other validation results. Before any of these claims are apportioned, the Service Provider will have the opportunity to seek review by submitting additional information that will allow the Purchaser to have another attempt at validation. Where the claim is not validated as a result of such review or the Service Provider does not request a review, this will contribute to the error rate for extrapolation.

Sustained Job Outcome Validation

1.20. Each month the Purchaser will randomly select for validation a sample (the size of the sample to be determined by the Purchaser) of claims which have been paid by the Purchaser to the Service Provider , that have been paid in the previous month for validation in respect of the second and the third KPIs. If the total of claims paid is less than the specified sample in any month then all will be selected. The Purchaser reserves the right to sample additional claims at any point in its absolute discretion. The Service Provider will be informed by the Purchaser of the Customers who have been selected within the sample.

1.21. The sample for Sustained Job Outcomes (26 weeks) will be subject to checks to establish if Customers have been in work for a minimum of 16 hours per week paid at NMW which has lasted 26 weeks out of 30 weeks. Breaks in employment must total no more than 4 weeks during the 30 week period as outlined in the second KPI.

1.22. The sample for Sustained Job Outcomes (52 weeks) will be subject to checks to establish if Customers have been in work for a minimum of 16 hours per week paid at NMW which has lasted 52 out of 60 weeks. Breaks in employment must total no more than 8 weeks during the 60 week period as outlined in the third KPI.

1.23. Where the Purchaser establishes that a Customer has not been in work for sufficient time when the claim is submitted to the Purchaser to meet the requirement but at the point of validation they have (and meet all requirements), the claim will be treated as a Technical Pass.

1.24. Where consent to contact the employer has been given but the employer is unable/unwilling to validate the claim, the Purchaser will contact the Customer. In cases where the Purchaser is experiencing difficulty making contact with the employer and/or the Customer, the Purchaser may, but is not obliged to, contact the Service Provider to confirm the details it has supplied. For example, where the Purchaser believes that the Service Provider has submitted incorrect or incomplete information (e.g. unobtainable telephone numbers). The Service Provider is required to establish the correct information and supply it promptly to the Purchaser to maximise the chances of positive contact during the validation window. If the Service Provider does not provide the detail that enables the Purchaser to validate the claim, the claim will fail validation.

1.25. Error rates are derived from checking a representative sample of claims and extrapolating against the remaining population of claims. This means the correct level of payment and performance will be attributed to a Service Provider. Therefore the Purchaser will not accept a request to withdraw a claim once a sample has been drawn.

1.26. There are four possible validation results:

• Pass – An employer/Customer confirms the condition for payment, as set out in the Sustained Job Outcome definition outlined in the Key Performance Indicators, has been met.

• Technical Pass – at the manual validation stage there are two scenarios:

- An employer/Customer confirms that there is a valid claim however the details provided by the employer and/or Customer differ from the details the Service Provider has supplied. The Purchaser will inform the Service Provider of the correct information and the Service Provider will update its records. The payment will not be recovered and will not contribute to the error rate for extrapolation.

- If the Purchaser establishes that a Customer has not been in work for a sufficient time within the claim period to meet the requirement but at the point of validation they have (and meet all other requirements), the claim will be treated as a Technical Pass. The payment will not be recovered and will not contribute to the error rate for extrapolation.

• Fail – An employer and/or Customer provides information which means the condition for payment, as set out in the Sustained Job Outcome definition, has not been met. The claim is recorded as an error and will contribute to the error rate for extrapolation.

• Unable to Validate – the Purchaser has either not been able to contact the employer/ Customer, or the employer and/or Customer are unable/ unwilling to provide the information required to validate the claim.

1.27. Unable to Validate claims will be apportioned across the other validation results. Before any of these claims are apportioned, the Service Provider will have the opportunity to seek review by submitting additional information that will allow the Purchaser to have another attempt at validation. Where the claim is not validated as a result of such review or the Service Provider does not request a review, this will contribute to the error rate for extrapolation.

1.28. Not used

Payment Validation Review Process (Outcomes and Sustained Job Outcomes)

1.29. Following the completion of the payment validation exercise, the Service Provider will receive a report from the Purchaser detailing the claims that have either failed and/or which the Purchaser has been Unable to Validate. This report will also give the information that informed the validation decision. Before any of these claims are used to calculate the error rate for extrapolation, the Service Provider will have 10 Working Days to consider this information and to submit additional information to the Purchaser. All requests for review, together with any supporting information or evidence, must be received within 10 Working Days of the validation failure report being provided to the Service Provider. Late requests will not be accepted and will be returned.

1.30. The Service Provider must ensure that requests for review are proportionate and reasonable and that additional information is provided to that supplied in the original claim that was not available at the time of the original submission. If the Purchaser is of the view that the additional information supplied allows the Purchaser to go back to an employer or Customer, another attempt to validate the outcome will be made by the Purchaser.

1.31. Where the original validation result failed because the Purchaser had been given information from an employer or Customer and/or employer that positively invalidates a claim, this is a fail and the Purchaser shall not attempt to revalidate the claim with the Customer.

1.32. Where the Service Provider has provided additional information that will allow the Purchaser to make additional enquires in the attempt to obtain a positive validation result, the Service Provider is shall email the Purchaser detailing all such relevant and appropriate information. The Service Provider may also provide physical evidence, however this will only be used in an attempt to revalidate the appropriate outcome, and will not be accepted in its own right. The Service Provider is shall submit any documentation to the Purchaser in line with Scottish Government security guidelines.

1.33. All requests for review, together with any supporting information or evidence, must be received within 10 Working Days of the validation failure report being sent to the Service Provider. Late requests will not be accepted and will be returned to the Service Provider. If no formal request has been received by the Purchaser by close of business on the 10th Working Day following the sending of such validation failure report, then cases which the Purchaser has been Unable to Validate or which have failed will be apportioned and an extrapolation report and invoice (if applicable) will be raised by the Purchaser. Such invoice shall be payable by the Service Provider to the Purchaser no later than 30 days from the date of the invoice.

1.34. Once the cases have been reviewed, the Purchaser will present the review findings to a review board. This board will have senior representation from the Purchaser. The purpose of the review board is twofold; to be satisfied that any reviewed decisions will stand up to scrutiny to the Purchaser's Internal Audit and Audit Scotland and to approve the original validation decision, if it remains unchanged. The review board may also request that the Purchaser or the Service Provider supply further information or investigation before finalising decisions.

1.35. Following approval from the review board, the Purchaser will notify the Service Provider of the results and issue the Service Provider with an extrapolation report. These decisions will have gone through a rigorous challenge process signed-off by senior representatives of the Purchaser to ensure that all valid claims are recognised. Decisions are final and no further challenge will be accepted.

1.36. Following a challenge, an unable to validate claim could be overturned to a Pass or a Fail. If it becomes a Fail, any such fails will contribute to the error rate for extrapolation.

1.37. The Purchaser operates regular review boards and extrapolation will be applied following the outcome of the review board.

Extrapolation Process Job Outcomes and Sustained Job Outcomes

1.38. The following paragraphs detail the extrapolation process. This process will be applied separately to payments made in respect of the first KPI and the second and third KPIs.

1.39. Following the review board decisions at the end of the relevant validation period, the number of Passes, Fails, Unable To Validates and Technical Passes, will be totalled for each monthly sample in the period. Claims that are positively invalidated contribute to the error rate for extrapolation.

1.40. A number of claims assessed to be Unable to Validate will be apportioned as fails. The number is calculated as follows:

a = number of Unable to Validate Outcomes
b = number of Outcome Fails
c = number of Outcome Technical Passes
d = number of Outcome Passes
e = denominator = b + c + d
f = total number of Outcome Payments in the sample = a + b + c + d
g = simple fail rate = b/f
h = Apportioned Unable to Validate Outcomes = a*b/e
(rounded to the nearest whole number),
I Total Outcome Fails = b+ h
Apportioned fail rate = i/f

1.41. The process for validation and extrapolation will be fully outlined within the Operational Guidance.

1.42 Where relevant, following such review, the Purchaser shall render an invoice in respect of the amount to be recovered as detailed in the extrapolation report as outlined in this Schedule. Such invoice shall be payable by the Service Provider to the Purchaser no later than 30 days from the date of the invoice.

Annex 2 – pricing breakdown

Implementation Costs – Not Applicable

Service Fees							
	Total Available Service Fee	**Year 1 Total Service Fee (50% of Total Available Service Fee for the service level**	**Year 1 Monthly Service Fee**	**Year 2 Total Service Fee (30% of Total Available Service Fee for the service level**	**Year 2 Monthly Service Fee**	**Year 3 Total Service Fee (20% of Total Available Service Fee for the service level)**	**Year 3 Monthly Service Fee**
	£	£	£	£	£	£	£
Core	[redacted]						
Advanced	[redacted]						
Intense	[redacted]						

Outcome Fees				
	Total available for outcomes (70% of Input Sheet Main Total for the service level) £	**Total Amount for Job Outcomes (15% of Total Available** £	**Total Amount for 1st Sustainment Payments (35% of total Available)** £	**Total Amount for 2nd Sustainment Payments (50% of total Available)** £
Core	[redacted]			
Advanced				
Intense				

Outcome Fees – Unit Cost			
	13 Week JO Payment £	**26 Week Sustainment Payment** £	**52 week Sustainment payment** £
Core	[redacted]	[redacted]	[redacted]
Advanced			
Intense			

Contingency Costs (refer to para 5.7 of Schedule 2)	
Costs based on clerical activity being the contingency	[redacted]

- Note: *Contingency Costs based upon 1 FTE over the full 4.25 years of the contract* [redacted] *a)) plus* [redacted] *of JMS development costs.*

This and the following 2 pages comprise Schedule 3 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 3 – CHANGE CONTROL PROCEDURES

1. CHANGE CONTROL PROCEDURES

1. General

1.1 Any change to the Contract shall be subject to the Change Control Procedures as set out below. For these purposes, a "**Change**" means any proposed amendment or change (including any proposed additional or substituted Schedules or Annexes), or any proposed change to the Services and/or the Contract.

1.2 The Purchaser may at any time request, and the Service Provider may at any time recommend a Change only in accordance with the Change Control Procedure as set out in this Schedule.

1.3 Neither Party shall unreasonably withhold its agreement to any Change. In the event that the Service Provider withholds its agreement to a Change, the Purchaser may, at its discretion perform the applicable Change itself where practicable at the Purchaser's cost.

1.4 Until such time as a Change is made in accordance with the Change Control Procedure, the Service Provider shall, unless otherwise agreed in writing by the authorised representatives of both Parties, continue to supply the Services as if the request or recommendation had not been made.

1.5 Any discussions which may take place between the Purchaser and the Service Provider in connection with a request or recommendation before the authorisation of a resultant Change shall be without prejudice to the rights of either Party.

1.7 Any work undertaken by the Service Provider or its subcontractor(s) which has not been agreed in accordance with the provisions of this Schedule shall be undertaken entirely at the expense and liability of the Service Provider.

1.8 For the avoidance of doubt, any Change which is necessary to ensure that the Services and any Deliverables meet the Specification and Service Levels (detailed at Schedule 1) shall be performed at no cost to the Purchaser.

2. Change Procedures

2.1 The Service Provider must have an appropriate structure and process in place to manage future developments, training, administration tasks and change requests from the Purchaser.

2.2 The Service Provider must acknowledge change requests received from the Purchaser within 2 Working Days. The Service Provider must be able to provide this in electronic and paper format. The Service Provider can follow up with the Purchaser if additional clarification is required regarding the Changes (s) and/or Service(s) requested.

2.3 Where either Party so requests, the Parties shall discuss a Change. Such discussion concerning a Change shall take place between the Purchaser and the Service Provider no later than ten (10) Working Days from either Party's request to discuss a Change unless the Parties agree otherwise. The discussion shall result in any one of the following:

(a) no further action being taken;
(b) a request to change the requirements of a Customer or the Services

2.4 Where a written request for an amendment (as outlined in the Request for Change Form included in this Schedule) is received from the Purchaser, the Service Provider shall, unless otherwise agreed, submit a CCN to the Purchaser within ten (10) Working Days of the date of the request which embodies substantially the terms of the request.

2.5 A recommendation to amend by the Service Provider shall be submitted as a CCN directly to the Purchaser at the time of such recommendation.

2.6 Each CCN shall contain:

(a) the title of the Change;
(b) the originator and date of the request or recommendation for the Change;
(c) the reason for the Change;
(d) full details of the Change including any amendments to the Contract including the Specification and the Pricing Schedule;
(e) the price, if any, of the Change and the Service Provider's methodology in arriving to such price (if relevant)
(f) effort in man days to implement the Change;
(g) a timetable for implementation together with any proposals for acceptance of the Change;
(h) a schedule of payments, if appropriate;
(i) details of the likely impact, if any, of the Change on other aspects of the Services to be provided including but not limited to:

i. the personnel to be provided;
ii. the payment profile;
iii. working arrangements;
iv. other contractual issues;

2.7 For each CCN submitted, the Purchaser shall, within the period of the validity of the CCN:

(a) allocate a sequential number to the CCN;
(b) evaluate the CCN and, where appropriate, request further information in relation to the Change and/or the CCN which further information shall be provided promptly by the Service Provider;
(c) approve the CCN;
(d) notify the Service Provider of the rejection of the CCN.

2.8 A CCN signed by both the Service Provider and the Purchaser shall subsequently constitute an amendment to the Contract. Work should not commence prior to both Parties' signature and any work carried out prior to such signature shall be at the Service Provider's cost.

2.9 Any potential Changes to either systems or processes will be presented to the Purchaser's Contract Manager (as may from time to time be appointed by the Purchaser) for approval to proceed.

3 Charges

3.1 The charges which apply to the Change will be as outlined in the CCN which has been approved by both Parties in accordance with paragraph 2.8. It is for the Service Provider to propose the applicable charges when producing the CCN in accordance with paragraph 2.6. The Parties (each acting reasonably) will discuss and endeavour to agree the charges for the Change which is being proposed.

This and the following 4 pages comprise Schedule 4 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 4 – MANAGEMENT ARRANGEMENTS

Governance

1. Contract Manager

1.1. The Purchaser's Contract Manager will be the main point of contact for the Service Provider.

1.2. The Purchaser's Contract Manager will manage the performance of the Service Provider including, but not limited to, the following:

- reviewing the overall management, operation and delivery of the Service Provider
- appraising the Service Provider against its KPIs and KDIs
- setting the strategic direction of the Service Provider's activities
- developing and implementing agreed marketing and communication approaches monitoring the cost-effectiveness of the operation of the Service Provider to ensure value for money
- responding to escalated key issues raised by the Service Provider or by the Purchaser in relation to the operation of and delivery under the contract, including, for example relating to performance, budget and other issues that are likely to have an impact upon the Purchaser's priorities and objectives.
- ensuring effective collaboration and links between the Purchaser and the Service Provider
- agreeing changes to the operation of the Service Provider

1.3. The Purchaser's Contract Manager will also receive the various performance reports as detailed below and as required in terms of the Contract. The Contract Manager may request relevant information from the Service Provider, as the need arises, and act as a key contract contact point for questions, proposals or requests from the Service Provider.

1.4. The Service Provider's Contract Manager will be the main point of contact for the Purchaser Contract Manager in relation to the Service Provider's performance of the Services. The Service Provide Contract Manager shall be responsible for liaising with the Purchaser Contract Manager in relation to all of the matters listed in paragraph 1.2 above (and shall provide all assistance and information requested by the Purchaser Contract Manager in relation to this. In addition, the Service Provider Contract Manager shall be responsible for supporting the strategic and day to day operation and management of the contract.

1.5 The Service Provider shall not change the Service Provider Contract Manager without Approval.

1.6 Office facilities for the Service Provider will not be provided by the Purchaser.

2. Reporting Arrangements

2.1 The Service Provider will report to the Purchaser on a range of aspects in relation to its performance under the Contract as outlined in paragraph 23 (Management Information) of Schedule 1 (Specification and Service Levels) on a regular basis as part of it meeting its requirements under the appointment.

3. Contract Review Meetings

3.1. In addition to the Contract Review Meetings as detailed in paragraph 39 (Contract Review Meetings) of Schedule 1 (Specification and Service Levels), during the first **three** months from the Effective Date (or longer as the Purchaser may consider necessary), there may be a requirement for ad-hoc meetings between the Purchaser's and the Service Provider's core team to discuss progress and identify any performance issues. All relevant current and pipeline projects will be discussed at these meetings, with a focus on those where there are issues to report and other relevant matters arising from time to time.

3.2. Written dashboards, or similar, outlining activity and progress against each Milestone will be provided by the Service Provider to the Purchaser in reasonable time priorto each meeting for consideration by the Purchaser's Contract Manager, and in any event not less than three Working Days prior to the meeting. This will form the basis for identifying any performance and/or compliance issues at an early stage.

3.3. Issues and risks will be discussed, and actions agreed and minuted by the Service Provider (such minutes to be provided to the Purchaser's Contract Manager for approval as agreed as soon as possible after the meeting or in any event no later than three Working Days prior to the next scheduled meeting).

4. Information Management / Performance Reporting

4.1 The format and content of the required management information will ultimately be agreed between the Purchaser and Service Provider, however in part the requested information as identified within paragraph 23 (Management Information) of Schedule 1 (Specification and Service Levels) may also include the following:

- Total value of sub-contracted spend in relation to the delivery of the Contract.
- Number of sub-contractors delivering goods or services in relation to the Contract.
- Confirmation that sub-contractor are paid within 30 days in accordance with the terms and conditions of the Contract. Reasons for any failure to comply.
- Number of SMEs delivering goods or services in relation to the Contract.
- Value of SME spend in relation to the Contract.
- Details of Health and Safety incidents relating to delivery of the Contract.

4.2 Reports are to be provided to the Purchaser on a (calendar) monthly basis, no later than 10 Working Days following the end of each month during the Contract Period.

4.3 All documents shall be submitted in electronic format and compatible with the Purchaser systems to enable access to and use of such documents by the Purchaser's Contract Manager as necessary.

4.4 Where the Service Provider fails to present a progress report or the final monitoring report and fails to furnish an acceptable written explanation of the reasons why it is unable to comply with this obligation, the Purchaser shall raise the issue via paragraph 6 below.

5. NOT USED

6. Dispute Resolution

6.1 The Parties shall attempt to resolve any dispute between them arising out of, or in connection with, this Contract within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute as follows.

6.2 Any dispute will, in the first instance, be presented to the Service Provider's Contract Manager and the Purchaser Contract Manager for resolution.

6.3 If the Service Provider's Contract Manager and the Purchaser Contract Manager cannot agree on a resolution, then a separate meeting will be held between the senior management of the Service Provider and the Purchaser for resolution.

6.4 If the dispute cannot be resolved by the Parties pursuant to this paragraph, the Parties shall refer it to mediation pursuant to the procedure set out at paragraph 6A to this Schedule unless:

a) the Purchaser considers that the dispute is not suitable for resolution by mediation;

or

b) the Service Provider does not agree to mediation.

6.5 The obligations of the Parties under this Contract shall not be suspended, cease or be delayed by the reference of a dispute to mediation and the Service Provider shall comply fully with the requirements of this Contract at all times.

6A. **Mediation**

6A.1 For the purposes of this mediation, the following terms are defined as follows:

"**CEDR**" means the Centre for Effective Dispute Resolution of International Dispute Resolution Centre, 70 Fleet Street, London EC4Y 1EU (www.cedr.com);

and

"**Contract Mediator**" means a neutral adviser or mediator chosen by agreement between the Parties.

6A.2. A Contract Mediator shall be appointed or, if the Parties are unable to agree upon a Contract Mediator within 10 Working Days after a request by one Party to the other or if the Contract Mediator agreed upon is unable or unwilling to act, either Party shall within 10 Working Days from the date of the proposal to appoint a Contract Mediator or within 10 Working Days of notice to either Party that he is unable or unwilling to act, apply to the CEDR to appoint a Contract Mediator.

6A.3. The Parties shall within 10 Working Days of the appointment of the Contract Mediator meet with him in order to agree a programme for the exchange of all relevant information and the structure to be adopted for negotiations to be held. If considered appropriate, the Parties may at any stage seek assistance from the CEDR to provide guidance on a suitable procedure.

6A.4. If the Parties reach agreement on the resolution of the dispute, the agreement shall be reduced to writing and shall be binding on the Parties once it is signed by their duly authorised representatives.

6A.5. Failing agreement, either of the Parties may invite the Contract Mediator to provide a non-binding but informative opinion in writing. Such an opinion shall be provided on a without prejudice basis and shall not be used in evidence in any proceedings relating to this Contract without the prior written consent of both Parties.

6A.6. If the Parties fail to reach agreement in the structured negotiations within 60 Working Days of the Contract Mediator being appointed, or such longer period as may be agreed by the Parties, then, for the purposes of clause 54.2 (Dispute Resolution), the dispute cannot be resolved in accordance with the Management Arrangements.

7. Continuous Service Improvement

7.1 Both Parties acknowledge the need for continuous improvement over the Contract Period as outlined in paragraph 28 (Continuous Improvement) of Schedule 1 (Specification and Service Levels) and that the Purchaser have paid the Service Provider for resources that are expected to deliver service improvement.

7.2 The Service Provider will deliver continuous improvement in the Services provided under this Contract, throughout the Contract Period.

7.3 The Service Provider recognises continuous improvement by following the 6 key principles of Scottish Government which are integral to creating a fairer Scotland (as defined within Annex A to Schedule 1).

7.4 Continuous improvement will be monitored by the Purchaser as part of the process for Service Provider management and review.

7.5 The Service Provider must put in place appropriate policies, processes, tools, methodologies and/or resources to continuously improve the service throughout the Contract Period and provide improved value for money.

7.6 During the Contract Period, the Service Provider shall be required to make proposals to the Purchaser which will:

a) improve the Service(s);

b) improve technology or methodology used in connection with the Services;

c) deliver Service efficiencies, reductions in whole-life costs and improvements in quality and performance.

7.7 The Service Provider must put in place a process to capture, assess, report and make recommendations to the Purchaser on initiatives and proposals for continuous improvement in the provision of the Services.

8. Complaints: Definition

8.1 Any communication from a Customer which meets any of the following criteria shall be classed as a complaint:

8.1.1 any communication identified by the Customer as a complaint;

8.1.2 any query or concern about the quality and/or performance of the Services received by the Customer;

8.1.3 any query or concern about any communications, or failure to communicate, through telephone, electronic means, letter or face to face, including the behaviour of anyone, involved in the delivery of the Services

("**Complaint**").

8.2 Where a Customer raises more than one Complaint relating to different areas of service or delivery, these shall be treated as separate Complaints.

9. Complaints: Handling

9.1 The Service Provider shall put in place a system for handling Complaints, which shall be defined and monitored centrally, be transparent, be easily accessible and be well publicised, as detailed in paragraph 18 (Feedback, Suggestions, Complaints and Escalation) of Schedule 1 (Specification and Service Levels).

10. Complaints: Resolution

10.1 The Service Provider shall adhere to the Complaints resolution process as outlined within paragraph 18 (Feedback, Suggestions, Complaints and Escalation) of Schedule 1 (Specification and Service Levels).

11. Complaints: Reporting

11.1 The Service Provider shall report monthly to the Purchaser on the number and nature of Complaints received, source of the Complaint, and the average time taken to resolve Complaints as detailed within paragraph 18 (Feedback, Suggestions, Complaints and Escalation) of Schedule 1 (Specification and Service Levels).

This and the following single page comprise Schedule 5 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 5 – KEY INDIVIDUALS

1. Operations Director [redacted]
2. Service Manager – T.B.A
3. Business Manager – T.B.A
4. Quality Assurance Manager – T.B.A
5. Integration Manager – T.B.A

Details to be provided by Service Provider following Contract Award.

This and the following single page comprise Schedule 6 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 6 – APPROVED SUB-CONTRACTORS

approved Sub-Service Provider(s)	**Relevant obligations**
1. Remploy Limited	Intense Service Strand
2. Momentum	Core and Advance Strand
3. The Lennox Partnership	Core and Advance Strand

This and the following 2 pages comprise Schedule 7 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 7 – SERVICE PROVIDER SENSITIVE INFORMATION

Type of information specified as Service Provider Sensitive Information	**Reason why information is sensitive**	**Duration of sensitivity**
1.1.3 Customer Journey - Stages	To release details of the names of our customer journey - stages would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.4 Customer Journey - Services Strand	To release details of the names of our customer journey – services strand would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.5 Proposed Delivery Mechanism	To release details of the names of our proposed delivery mechanism would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.6 Appendix 1 - Supply Chain Split Remove contact names.	To release details of the names of our contacts in the supply chain would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.7 Part 6 of ITT - Subcontractor Declarations Remove contact names.	To release details of the names of our contacts in the supply chain would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.9 Delivery Locations Remove contact names and locations.	To release details of the names of our contacts and their delivery locations would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.10 Appendix 2 - Subcontractor Locations and Facilities Remove contact names and locations.	To release details of the names of our contacts names and locations would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.12 Stakeholder Engagement Remove contact names.	To release details of the names of our contacts would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.

Type of information specified as Service Provider Sensitive Information	Reason why information is sensitive	Duration of sensitivity
1.1.13 Appendix 3 - Stakeholder Engagement Plan Remove contact names.	To release details of the names of our contacts would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.15 Employer Engagement Remove contact names.	To release details of the names of our contacts would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.2.1 Management Structure	To release details of our management structure would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.2.2 Staffing Resources / Proposals to Ensure Robust Delivery	To release details of our staff resources would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.2.3 Resource Plans	To release details of our staff resources would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.3.1 Performance Offer	To release details of the names of our performance offer would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.5.2 Performance Management	To release details of the names of our performance management processes would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
Commercial Envelope – Tender price	To release details of our tender price would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
Commercial Envelope – Commercial Questionnaire	To release details of the names of our commercial questionnaire would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.

This and the following single page comprises Schedule 8 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 8 – PARENT COMPANY GUARANTEE

NOT USED

This and the following 13 pages comprise Schedule 9 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 9 – MODEL CONTRACT REGARDING DATA PROTECTION DIRECTIVE 95/46/EC

Model Contract

STANDARD FORM CONTRACT TO ASSIST COMPLIANCE WITH OBLIGATIONS IMPOSED BY ARTICLE 17 OF THE DATA PROTECTION DIRECTIVE 95/46/EC

(FOR USE BY DATA CONTROLLERS AND DATA PROCESSORS LOCATED WITHIN THE EUROPEAN ECONOMIC AREA WHERE THE PARTIES HAVE ENTERED INTO A SEPARATE DATA PROCESSING AGREEMENT)

THIS AGREEMENT is made on……and ……20[ ].

BETWEEN:

(1) THE SCOTTISH MINISTERS (the "Controller"); and

(2) PeoplePlus Group Limited (incorporated in, or existing and established under the laws of, United Kingdom (Company registered number 05722765) whose registered office is at 19-20 The Triangle, Ng2 Business Park, Nottingham, NG2 1AE (the "Processor").

BACKGROUND

(A) The Controller processes Personal Data in connection with its business activities;

(B) The Processor processes Personal Data on behalf of other businesses and organisations;

(C) The Controller wishes to engage the services of the Processor to process personal data on its behalf in relation to **Fair Start Scotland**;

(D) Article 17(2) of the Data Protection Directive 95/46/EC (as hereinafter defined) provides that, where processing of personal data is carried out by a processor on behalf of a data controller the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;

(E) Articles 17(3) and 17(4) of the Data Protection Directive require that where processing is carried out by a processor on behalf of a controller such processing shall be governed by a contract or legal act binding the processor to the controller stipulating, in particular, that the processor shall act only on instructions from the controller and shall comply with the technical and organisational measures required under the appropriate national law to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing;

(F) In compliance with the above-mentioned provisions of Article 17 of the Data Protection Directive the
Controller and Processor wish to enter into this processing security Agreement.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"**Data Protection Directive**" shall mean Directive 95/46/EC of the European Parliament and Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"**national law**" shall mean the law of the Member State in which the Processor is established;

"**personal data**" shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

"**processing of personal data**" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

"**sub-contract**" and "**sub-contracting**" shall mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and "Sub Contractor" shall mean the party to whom the obligations are subcontracted; and

"**Technical and organisational security measures**" shall mean measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure oraccess and against all other unlawful forms of processing.

2. CONSIDERATION

2.1 In consideration of the Controller engaging the services of the processor to process personal data on its behalf the Processor shall comply with the security, confidentiality and other obligations imposed on it under this Agreement.

3. SECURITY OBLIGATIONS OF THE PROCESSOR

3.1 The Processor shall only carry out those actions in respect of the personal data processed on behalf of the Controller as are expressly authorised by the Controller.

3.2 The Processor shall take such Technical and Organisational Security Measures as are required under its own national law to protect personal data processed by the Processor on behalf of the Controller against unlawful forms of processing. Such Technical and Organisational measures shall include, as a minimum standard of protection, compliance with the legal and practical security requirements set out in Appendix 1 of this Agreement.

4. CONFIDENTIALITY

4.1 The Processor agrees that it shall maintain the personal data processed by the Processor on behalf of the Controller in confidence. In particular, the Processor agrees that, save with the prior written consent of the Controller, it shall not disclose any personal data supplied to the Processor by, for, or on behalf of, the Controller to any third party.

4.2 The Processor shall not make any use of any personal data supplied to it by the Controller otherwise than in connection with the provision of services to the Controller.

4.3 The obligations in clauses 4.1 and 4.2 above shall continue for a period of five years after the cessation of the provision of services by the Processor to the Controller.

4.4 Nothing in this agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

5. SUB-CONTRACTING

5.1 The Processor shall not sub-contract any of its rights or obligations under this Agreement without the prior written consent of the Controller.

5.2 Where the Processor, with the consent of the Controller, sub-contracts its obligations under this agreement it shall do so only by way of a written agreement with the Sub-Contractor which imposes the same obligations in relation to the security of the processing on the Sub-Contractor as are imposed on the Processor under this Agreement.

5.3 For the avoidance of doubt, where the Sub-Contractor fails to fulfil its obligations under any sub-processing agreement, the Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this Agreement

6. TERM AND TERMINATION

6.1 This Agreement shall continue in full force and effect for so long as the Processor is processing personal data on behalf of the Controller.

6.2 Within [insert the number of days agreed by the parties] days following termination of this Agreement the Processor shall, at the direction of the Controller, (a) comply with any other agreement made between the parties concerning the return or destruction of data, or (b) return all personal data passed to the Processor by the Controller for processing, or (c) on receipt of instructions from the Controller, destroy all such data unless prohibited from doing so by any applicable law.

7. GOVERNING LAW

7.1 This Agreement shall be governed by and construed in accordance with the national law of the Member state in which the Controller is established.

AS WITNESS this Agreement has been signed on behalf of each of the parties by its duly authorised representative on the day and year first above written.

SIGNED on behalf of [CONTROLLER]

(Authorised signatory)

(Print name and title)

SIGNED on behalf of [PROCESSOR]

(Authorised signatory)

(Print name and title)

APPENDIX 1[1]

1. Legal requirements

1.1 The Processor shall, in respect of the processing of personal data on behalf of the Controller, identify and comply with any specific security provisions imposed by its national law.

2. Practical security measures

2.1 In compliance with its obligations under clause 3.2 with regard to the processing of personal data on behalf of the Controller, the Processor, as a minimum requirement, shall give due consideration to the following types of security measures:

2.1.1 Information Security Management Systems;

2.1.2 Physical Security;

2.1.3 Access Control;

2.1.4 Security and Privacy Enhancing Technologies;

2.1.5 Awareness, training and security checks in relation to personnel;

2.1.6 Incident/Response Management/Business Continuity; and

2.1.7 Audit Controls/Due Diligence;

---

1 The Practical Security Measures outlined in Schedule 1 are taken from the OECD Working Party on Information Security and Privacy's draft paper of 30-31March 2004 entitled "Information Security Issues and Resources for Small and Entrepreneurial Companies – A business companion to the 2002 OECD Guidelines for the Security of Networks and Information systems: Towards a Culture of Security"

Annex A (normative):

Article 17 Security Contract - Implementation Guide

AA.1 **Scope**

The Article 17 Security Contract has been prepared to assist businesses wishing to use the services of another company to process personal data on their behalf. The Article 17 Security Contract is appropriate for use where the company which is to provide the data processing service is located either in the same Member State as the business wishing to use its services or, is located another Member State of the European Union.

Article 17 of the Directive sets out the security requirements in relation to the processing of personal data where a party that controls the content and use of personal data (the Data Controller) wishes to use the services of a third party (the Data Processor) for the processing of such data. Article 17 addresses processing arrangements where both the Data Controller and the Data Processor are established within one of the member states of the European Economic Area.

Where the Data Processor is located outside the European Economic Area consideration will need to be given to the provisions of Articles 25 and 26 of the Directive (Transfer of Personal Data to Third Countries) and the possible use of the Standard Contractual Clauses for the transfer of personal data to third countries under the Directive approved by the European Commission.

The Article 17 Security Contract has been prepared with the needs of Small and Medium-sized Enterprises in mind, however, it may in addition provide a useful starting point for larger organisations wishing to ensure that they are satisfying their obligations as to security of processing where they sub-contract data processing to another company.

The Article 17 Security Contract has been drafted to satisfy the requirements of Article 17 and is unlikely to
require amendment in the absence of any changes to that Article. The contractual provisions set out in the Security Contract ensure the basic minimum level of protection for personal data and do not preclude the inclusion of more detailed provisions in the light of the legal and factual circumstances of each particular case.

However, the practical security measures suggested in this Implementation Guide are likely to require amendment in the light of physical and technological security developments and the adoption of enhanced management functions in relation to information security. This Implementation Guide, therefore, sets out the current practical security measures identified at the time of drafting, taking into account the most common technical security measures currently available, but may subsequently require updating to incorporate future developments.

The Article 17 Security Contract is designed to accompany a service agreement detailing the non-security related processing arrangements between the Data Controller and the Data Processor. The Contract may be used in its entirety or the operative clauses may be extracted and incorporated into the processing service agreement.

Before entering in an Article 17 Security Contract, or the data processing services agreement into which the operative of the Security Contract have been incorporated, the parties should obtain the assistance of professional legal advisers (in-house or external lawyers) for advice on the requirements of the national law (including any sector specific regulatory arrangements) to which the contract and the associated processing will be subject.

This guide provides assistance with regard to the use of the Article 17 Security Contract between Data Controller and Data Processor.

AA.2 **Background**

The Initiative for Privacy Standardisation in Europe (IPSE) was launched to analyse the current status of privacy protection arrangements and to determine whether standardisation of actions could assist business in implementing the European Data Protection Directive 95/46/EC (the Directive). The report, approved by the IPSE steering group, concluded that specific standardisation initiatives would aid implementation of the Directive. Seven standardisation initiatives were proposed, one of which was the development of a generic set of contract clauses and terms for use within the EEA to assist business in complying with Article 17 of the Directive.

The work on the standardisation initiatives identified by IPSE was taken on by the CEN/ISSS Work Shop on Data Protection and Privacy (CEN/ISSS WS-DPP) which has produced the Article 17 Security Contract between Data Controller and Data Processor.

AA.3 **Applicable Laws**

Clause 6 of the Security Contract provides that the Agreement is to be governed by the national law of the Member State in which the Data Controller is located.

Where the Data Processor is located in a different Member State from the Data Controller the Controller should note that the security of the processing may be governed by the laws of a different Member State. This situation arises as (in accordance with the provisions of Article 17) the security of the processing must be conducted in accordance with the national law of the Member State in which the Data Processor is located.

Where the Data Processor is located in a Member State other than that of the Data Controller, prior to entering into contractual relations with the Data Processor, the Data Controller may need to obtain legal advice as to the specific foreign law data protection obligations imposed on the Data Processor under Clause 3 of the Model Contract. Where the Data Controller fails to obtain foreign legal advice the Data Controller may struggle to assess the Data Processor's compliance with its Clause 3 obligations. While the obligations of the Data Processor, in each Member State, derive from Article 17 of the Directive, Member States have each implemented these obligations slightly differently. For example, in many Member States (such as Austria, Belgium, Ireland, Italy, Luxembourg and Spain) the security provisions under the national law are more detailed than in the Data Protection Directive. The Data Processor will, therefore, need ensure that it complies with the provisions under the applicable national law.

In certain Member States there are regulations detailing mandatory security measures which identify three differing levels of security determined by the nature of the data being processed.

High level security measures required in Spain include, amongst other requirements, strict obligations regarding the encryption of personal data in specified circumstances as well as the maintenance of an exhaustive access registry. The Spanish access register requires a Controller to specify the data accessed by any user and the date and time of such access so as to enable the reconstruction of an audit trail in relation to access to sensitive personal data.

In Belgium, national data protection legislation stipulates and number of issues that must be covered in any sub-contracting agreement between Data Controller and Data Processor. Such issues include a requirement that the agreement shall explicitly include details of the processors liability under the agreement. The Belgium law also provides that a Royal Decree may be enacted to establish standards for information security for specified categories of data processing.

In Greece the national data protection law requires the Data Controller to check the professional credentials, qualifications and personal ethics with regard to confidentiality of persons entrusted with data processing duties or functions.

In addition to these specific national legal requirements some national data protection authorities (for example Greece and Denmark) have established rules, instructions and guidelines translating into more practical terms some of the requirements of Article 17.

AA.4 Clause by clause explanatory notes/analysis of the Article 17 Security Contract

As with any arrangement having binding legal effect, users of the Article 17 Security Contract are advised to seek professional legal advice with regard to their rights and obligations under the Security Contract and its inter relationship with any associated data processing service agreement.

Professional legal input is particularly important where the Data Controller is uncertain of the obligations imposed on the Data Processor under the Processor's national law.

The following notes are intended as basic guidance on the nature and purpose of the individual clauses of the Security Contract and are intended to inform business managers understanding of the Security Contract prior to obtaining detailed legal advice.

Contract Clauses

Date of Agreement

The date of the agreement will be the date on which the last party executes the document. This date should not be inserted until the last party has signed and dated the Contract.

Identification of Parties

The full name of the legal entities entering into the agreement should be inserted together with any nationalcompany registration number, details of the country in which each legal entity is established and details of the registered office of each entity. It is important to note that address must be the registered office address of each business. Trading addresses, or local office addresses should not be used.

Background

The six paragraphs listed under this heading set out the reasons why the agreement is required. They identify the activities of the parties, the processing of personal data, the parties who wish to enter into contractual relations with one another, and the requirements of Article 17 of the Directive.

Mutual Agreement

The Contract then states that the parties agree to comply the provisions of the Contract.

Clause 1 – Definitions and Interpretation

This clause explains the meaning of those terms used in the agreement which have meaning over and above, or different from, the meaning which may normally be understood by the use of the term. For example, the words "personal data" are to have the specific meaning ascribed to them by the Directive.

Clause 2 – Consideration

Broadly speaking this clause is required to set out the reasons why each party is prepared to enter into the agreement. The Contract arrangement needs to be of benefit to (or, in legal terms, provide valid consideration) each party.

Clause 3 – Security Obligations of the Processor

As the title of this clause would suggest, it sets out the security obligations of the Data Processor with regard to the processing of personal data on behalf of the Data Controller.

Important points to note are:

- the Processor may only process personal data in accordance with instructions from the Data Controller. It may not process the data for its own purposes;

- the Processor is required to take “such Technical and Organisation Security Measures as are required under **its own National Law** to protect personal data processed on behalf of the Data Controller against unlawful forms of processing”. As mentioned above, legal advice should be obtained as to the detailed requirements of the relevant national law; and

- Appendix 1 of the Contract sets out the minimum requirements for compliance with these obligations. Appendix 1 is discussed further below.

Clause 4 – Confidentiality

This clause ensures that the Processor must treat all personal data processed on behalf of the Data Controller as confidential and provides that the obligation of confidentiality is continue for 5 years after the date on which the Processor ceases processing personal data for the Controller. This time limit is without prejudice to any longer time-limits that may be provided by national law or sector specific regulation. The parties may wish to amend this provision to reflect such additional obligations.

Clause 5 – Sub-contracting

This clause prevents the Processor from instructing a third party to carry out the processing it has agreed to carry out for the Controller unless the Controller gives its prior written consent.

Where the Controller consents to the sub-contracting, the sub-contractor must be contractually bound to observe the same security requirements as are imposed on the Processor under the Security Contract.

This clause ensures that the security arrangements are not watered-down by any transfer of obligations. The clause also provides that the Processor remains liable to the Controller for any breach of the Security Contract whether caused by any fault of its own or by the fault of its sub-contractor.

Clause 6 – Term and termination

This clause provides that the Security Contract will continue for as long as the Processor continues to process personal data on behalf of the Controller. The Security Contract cannot terminate before the data processing service agreement as any subsequent processing would not comply with Article 17.

Where the Security Contract and the data processing agreement are terminated, clause 5.2 provides that the Processor shall return or destroy all personal data received from the Controller as instructed by the Controller. It is for the parties to agree the appropriate number of days to insert in the clause.

This arrangement is fallback position to specify arrangements for the handling of the personal data on termination where there are no other arrangements in place. It is highly likely that the termination arrangements will be addressed in the data processing service agreement but clause 5.2 is available as backup if such arrangements have been overlooked in the drafting of the service agreement.

Clause 7 – Governing law

The Security Contract provides that the contract is to be governed by the National Law of the Data Controller.

Care must be taken when considering the choice of governing law in circumstances where the data processing service agreement specifies a law other than that of the Member State of the Controller as its governing law. In such circumstances professional legal advice may be required.

The Security Contract does not address dispute resolution. It is advisable, before the Contract is signed, for the parties to agree an appropriate forum to hear any disputes that may arise between them under the Contract. Many parties may favour mediation with recourse to specified national courts if matters cannot be resolved. Others may wish to specify arbitration as the preferred dispute resolution process. Where mediation or arbitration are to be used it is advisable to identify the chosen mediator (or mediation body) or arbitration procedure in writing so as to avoid a dispute about the Contract becoming a dispute about the resolution procedure.

As the Security Contract is to be used in association with a data processing service agreement it may be appropriate to deal with dispute resolution arrangements in relation to security obligations under the service agreement or to mirror the dispute resolution arrangements under the service agreement in the Security Contract. Where mediation or arbitration is not specified, as a minimum, the parties should agree to submit to the exclusive jurisdiction of specified national courts to avoid any further discussion as to where disputes should be heard. It is usual for parties to agree to submit to the exclusive jurisdiction of the courts appropriate to the governing law of the contract.

Signature

Both parties should ensure that the Contract is executed on their behalf by a 'duly authorised representative'. That is to say the parties should ensure that the signatories have the power to bind the organisation they represent. In many jurisdictions, in the absence of any other arrangements being made, the only individuals authorised to bind a company will be the directors and company secretary. These individuals may of course give written authority to other employees to bind the company for specified purposes. The identity and the authority of the proposed signatory should always be confirmed before attempting to enter into contractual relations.

Appendix 1

This appendix sets out the minimum technical and organisational measures to be observed by the Processor in accordance with clause 3. The appendix is divided into Legal Requirements and Practical Security Measures.

The Legal Requirements

These relate to the need for the Data Processor to identify and observe any specific security measures in relation to personal data required under its national law. The requirement is not a one-off requirement to be observed at the start of the processing service, but is an on-going obligation to ensure that the security arrangements are in compliance with national law as it may be amended or supplemented from time to time throughout the duration of the processing service.

Practical Security Measures

While the Contract imposes the obligation on the Processor to take "such Technical and Organisation
Security Measures as are required under its own National Law to protect personal data processed on behalf of the Data Controller against unlawful forms of processing" many businesses may find it difficult to ascertain what this obligation means in practice.

The obligation is a broad one and businesses will need to break this down into the classes of security measures identified in the appendix. These classes will require further practical consideration. Many international IT groups and standards bodies have looked at the area of information security and guidance of general application is available from many of the bodies referred to below (see Sources).

An example of appropriate basic information security measures are set out in Annex 1 of this Implementation Guide.

AA.5 Extra Clauses
The Security Contract (whether used as an separate agreement or with extracted clauses used to supplement a data processing agreement) is intended to satisfy the requirements of Article 17.

From a business perspective, however, where such matters have not been otherwise covered in the data processing agreement or related contract, parties may wish to include additional clauses regarding, for example:

- Arbitration or mediation arrangements (as discussed above);
- Selection of jurisdiction (as discussed above);
- Limitations of liability.

Where more detailed arrangements have not been dealt with in other agreements, parties may wish to include more detailed provisions in relation to some of the matters addressed in the Security Contract, for example:

- Arrangements for the treatment of personal data on termination of the processing arrangements.

AA.6 Sources
The following bodies provide helpful guidance and information on information security, privacy enhancing
technologies and data protection and privacy considerations which may serve as useful additional reading material for organisations seeking to use the Article 17 Security Contract for the first time:

- OECD/EU
- National Bodies
- BCS, ITIL
- ICC (International Chamber of Commerce)
- ISO 17799
- Common Criteria
- PETTEP

IMPLEMENTATION GUIDE

ANNEX 1 - BASIC INFORMATION SECURITY MEASURES

Basic information security measures (here extracted from work of the OECD) will include consideration of the following:

2.1 Information Security Management System/Privacy and Data Protection Management System

- Policy
- Governance
- Process/procedures
- Roles/responsibilities
- Assurance process
- Risk Assessment
- Improvement plan.

2.2 Physical Security

- Fit appropriate locks or other physical controls to the doors and windows of rooms where computers are kept.
- Physically secure unattended lap tops (for example, by locking them in a secure drawer or cupboard).
- Ensure you control and secure all removable media, such as removable hard-drives, CDs, floppy disks and USB drives, attached to business-critical assets.
- Destroy or remove all business-critical information from media such as CDs, and floppy disks before disposing of them.
- Ensure that all business-critical information is removed from the hard drives of any used computers before disposing of them.
- Store back-ups of business-critical information either off-site or in a fire and water-proof container.

2.3 Access Controls

- Use unique passwords, that are not obvious *(*Note: not birth dates or easily found or guessed information*)* and change them regularly *(*Note: preferably at least every three months*).*
- Use passwords that contain letters in both upper and lower cases, numbers and special keys, and are six or more characters in length. (Note: Passwords remembered as a memorable sentence, rather than a single word, are helpful. For example, the sentence: "at forty-two I'm a star!" can translate into this eight-character password : @42Ima**!)***
- Ensure that employees don't write down or share passwords. *(*Note: If an employee finds that they need, on occasion, to share a password they must be required to change it as soon as possible – no matter how well they trust the person they shared it with!*)*

2.4 Security and Privacy Technologies

- Ensure that all computers used have anti-virus software installed, and the virus definitions must be updated at least once a week *(*Note: many providers have a one-click update*).* Allincoming and outgoing traffic must be scanned for viruses, as should any disk or CD that is used, even if it is from a 'trusted' source. At least once a month, computers must be scanned for viruses.

- Where computers are connected to the Internet (especially if you use a broadband connection) deploy a software firewall. *(*Note: This helps to prevent malicious code from entering computers and potentially compromising the confidentiality, integrity and availability of a network. It also helps to stop a system being used to attack other systems without the system owner's knowledge. Software firewalls for use by non-professionals are readily available at a reasonable cost. Operating system virus control software or ISPs may also offer firewalls. Consumer and popular trade magazines compare firewall functions and features of well known products, and are a good source of information. Free shareware firewalls are available, but these usually require expert knowledge for correct use*).*

- Where a business has a small network that is connected to the Internet, it should consider deploying an 'all-in-one' hardware box that contains a firewall, anti-virus program and an intrusion detection system. *(*Note: This will greatly simplify the use and maintenance of essential Internet security technology*).*

2.5 Awareness, training and security checks in relation to personnel

- Perform integrity checks on all new employees to ensure that they have not lied about their background, experience or qualifications.
- Give all new employees a simple introduction to information security, and ensure that they read and understand your information security policy. Ensure employees know where to find details of the information security standards and procedures relevant to their role and responsibilities.
- Ensure that employees have access only to the information assets they need to do their jobs. If employees change jobs, you must ensure that they do not retain access to the assets they needed for their old job. When dismissing employees, ensure that they do not take with them any business-critical information.
- Ensure that no ex-employees have access rights to your systems.
- Ensure employees know about the common methods that can be used to compromise your system. *(*Note: These include e-mail messages that contain viruses and 'social engineering' ploys used by hackers to exploit employees' helpfulness to gain information that will give them access to a system. Examples of 'social engineering' include a hacker using the telephone to pose as a systems maintenance engineer or pretending to be a new employee*).*

2.6 Incident/Response Management/Business Continuity

- Ensure that employees understand what is meant by a Security Incident. A security incident is any event that can damage or compromise the confidentiality, integrity or availability of your business–critical information or systems.

- Ensure that employees are trained to recognise the signs of Security Incidents. (*Note: These could include:*

    - strange phone requests, especially for information
    - unusual visitors
    - strange patterns of computer activity
    - unusual appearance of computer screens
    - computers taking longer than usual to perform routine tasks*)*

- Ensure that employees receive training on the need to notify anything which may be a sign of a Security Incident and are kept informed as to the identity of the person to whom such notifications should be made.
- Ensure that if a Security Incident occurs, employees know who to contact and how.
- Have in place a plan to assure business continuity in the event of a serious Security Incident (a "Business Recovery Plan"). The plan should specify:
- Designated people involved in the response;
- External contacts, including law enforcement, fire and possibly technical experts;
- Contingency plans for foreseeable incidents such as:
    - Power loss;
    - Natural disasters and serious accidents;
    - Data compromise;
    - No access to premises;
    - Loss of essential employees;
    - Equipment failure;

- Ensure that your Business Recovery Plan is issued to all employees and is tested at least once a year, regardless of whether there has been a Security Incident.
- After every incident when the plan is used, and after every test, re-examine and update the Business Recovery Plan as necessary using the lessons learned.

2.7 Audit Controls/Due Diligence

Ensure that you have in place appropriate security audit arrangements including:

- Auditing of who has access to its system (in general and in relation to particular types of information) *(*Note: The ability to audit and evaluate information security compliance is essential – you can't manage what you don't measure!*);*
- Logging of such access to the system; and
- Auditing of compliance with security procedures. *(*Note: A record should be maintained for each security procedure. For example, if a procedure requires that you test your system's back-up generator once a week, an employee should be identified to sign a record to show that this has been done. Keeping good records is essential to audit control*.)*

Some audit controls may be necessary for legal or regulatory purposes. Good record keeping will clearly demonstrate compliance with obligations.

An audit should ensure that the procedures in place are effective and relevant. A security audit is a trigger to re-assess and re-evaluate the effectiveness of information security standards and procedures.

Audits are only effective if action is taken to address their findings and identify and implement the steps that need to be taken. A good audit trail is not just a paper exercise. If something goes wrong, the trail should identify what happened and why. This will help to keep improving the security of the business systems.

ANNEX 1: DATA SHARING PROTOCOL

[NOTE: DATA SHARING PROTOCOL TO BE INSERTED FOLLOWING CONTRACT AWARD DEPENDING ON DATA TRANSFER REQUIREMENTS AND DETAILS BEING FINALISED.]

This and the following 10 pages comprise Schedule 10 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 10 – EXIT MANAGEMENT

1. **DEFINITIONS**

1.1 In this Schedule, the following definitions shall apply:

"**Exclusive Assets**" means those Service Provider Assets used by the Service Provider or a Key Sub-Contractor which are used exclusively in the provision of the Services;

"**Exit Information**" has the meaning given to it in paragraph 4.1 of this Schedule;

"**Exit Manager**" means the person appointed by each Party pursuant to paragraph 3.4 of this Schedule for managing the Parties' respective obligations under this Schedule;

"**Key Sub-Contractor**" means each Sub-contractor listed in Schedule 6 and any additional sub-contractors who are notified to and approved by the Purchaser pursuant to the Contract;

"**Net Book Value**" means the net book value of the relevant Service Provider Asset(s) calculated in accordance with the depreciation policy of the Service Provider set out in the letter in the agreed form from the Service Provider to the Purchaser of even date with this Contract;

"**Non-Exclusive Assets**" means those Service Provider Assets (if any) which are used by the Service Provider or a Key Sub-Contractor in connection with the Services but which are also used by the Service Provider or Key Sub-Contractor for other purposes;

"**Purchaser Data**" means any data (including any Personal Data (as defined in section 1(1) of the Data Protection Act 1998) relating to the staff, customers or suppliers of the Purchaser), documents, text, drawings, diagrams, images or sounds (together with any database made up of any of those), embodied in any medium, that are supplied to the Service Provider by or on behalf of the Purchaser, or which the Service Provider is required to generate, process, store or transmit pursuant to the Contract;

"**Purchaser Software**" means any software which is used by, or licensed to, the Purchaser other than pursuant to the Contract, and which may be used by the Service Provider for the sole purpose of providing the Services to the Purchaser;

"**Registers**" means the register and configuration database referred to in paragraphs 3.1.1 and 3.1.2 of this Schedule;

"**Service Provider Assets**" means all assets and rights of the Service Provider which are required to provide any of the Services in accordance with the Contract;

"**Sub-Contracts**" means any contract between the Service Provider and a third party pursuant to which the Service Provider agrees to source the provision of any of the Services from that third party;

"**Termination Assistance**" means the activities to be performed by the Service Provider pursuant to the Exit Plan, and any other assistance required by the Purchaser pursuant to the Termination Assistance Notice;

"**Termination Assistance Notice**" has the meaning given to it in paragraph 6.1 of this Schedule;

"**Termination Assistance Period**" means in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Service Provider is required to provide the Termination Assistance as such period may be extended pursuant to paragraph 6.2 of this Schedule;

"**Termination Notice**" a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Contract (in whole or in part) on a specified date and setting out the grounds for termination.

"**Third Party Software**" means software which is proprietary to any third party and that is either licensed to the Purchaser or is used by the Service Provider in the provision of the Services, but excluding any Purchaser Software;

"**Transferable Assets**" means those of the Exclusive Assets which are capable of legal transfer to the Purchaser;

"**Transferable Contracts**" means the Sub-Contracts, licenses for Service Provider 's software, licenses for Third Party Software or other agreements which are necessary to enable the Purchaser or any Replacement Service Provider to perform the Services (or any replacement to the Services), including in relation to licenses all relevant Documentation;

"**Transferring Assets**" has the meaning given to it in paragraph 9.2.1 of this Schedule;

"**Transferring Contracts**" has the meaning given to it in paragraph 9.2.3 of this Schedule.

2. **INTRODUCTION**

2.1 This Schedule describes provisions that should be included in the Exit Plan, the duties and responsibilities of the Service Provider to the Purchaser leading up to and covering the transfer of service provision to the Purchaser and/or a Replacement Service Provider.

2.2 The objectives of the exit planning and service transfer arrangements are to ensure a smooth transition of the availability of the Services (in whole or in part) from the Service Provider to the Purchaser and/or a Replacement Service Provider.

3. **OBLIGATIONS DURING THE CONTRACT PERIOD TO FACILITATE EXIT**

3.1 During the Contract Period, the Service Provider shall:

3.1.1 create and maintain a Register of all:

(a) Sub-Contracts and other relevant agreements (including relevant software licenses, maintenance and support agreements and equipment rental and lease agreements) required for the performance of the Services; and

(b) Exclusive Assets and Non-Exclusive Assets.

3.1.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Service Provider provides the Services, which shall contain sufficient detail to permit the Purchaser and/or Replacement Service Provider to understand how the Service Provider provides the Services and to enable the smooth transition of the Services with the minimum of disruption;

3.1.3 agree the format of the Registers with the Purchaser as part of the process of agreeing the Exit Plan; and

3.1.4 at all times keep the Registers up to date, in particular in the event that Assets (whether Exclusive or Non-Exclusive), Sub-Contracts or other relevant agreements are added to or removed from the Services.

3.2 The Service Provider shall:

3.2.1 procure that all Exclusive Assets listed in the Registers are clearly marked to identify that they are exclusively used for the provision of the Services under this Contract; and

3.2.2 (unless otherwise agreed by the Purchaser in writing) procure that all licenses for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation at the request of the Purchaser to the Purchaser (and/or its nominee) and/or any Replacement Service Provider upon the Service Provider ceasing to provide the Services (or part of them) without restriction (including any need to obtain any consent or approval) or payment by the Purchaser.

3.3 Where the Service Provider is unable to procure that any Sub-Contract or other agreement referred to in paragraph 3.2.2 of this Schedule which the Service Provider proposes to enter into after the Effective Date is assignable and/or capable of novation to the Purchaser (and/or its nominee) and/or any Replacement Service Provider without restriction or payment, the Service Provider shall promptly notify the Purchaser of this and the Parties shall (acting reasonably and without undue delay) discuss the appropriate action to be taken which, where the Purchaser so directs, may include the Service Provider seeking an alternative Sub-Contractor or provider of goods and/or services to which the relevant agreement relates.

3.4 Each Party shall appoint a person (the "**Exit Manager**") for the purposes of managing the Parties' respective obligations under this Schedule and provide written notification of such appointment to the other Party within three (3) months of the Effective Date. The Service Provider's Exit Manager shall be responsible for ensuring that the Service Provider and its employees, agents and Sub-Contractors comply with this Schedule. The Service Provider shall ensure that its Exit Manager has the requisite authority to arrange and procure any resources of the Service Provider as are reasonably necessary to enable the Service Provider to comply with the requirements set out in this Schedule. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the termination of this Contract and all matters connected with this Schedule and each Party's compliance with it.

4. **OBLIGATIONS TO ASSIST ON RE-TENDERING OF SERVICES**

4.1 On reasonable notice at any point during the Contract Period, the Service Provider shall provide to the Purchaser and/or its potential Replacement Service Providers (subject to the potential Replacement Service Provider s entering into reasonable written confidentiality undertakings), the following material and information in order to facilitate the preparation by the Purchaser of any invitation to tender and/or to facilitate any potential Replacement Service Providers undertaking due diligence:

4.1.1 details of the Service(s);

4.1.2 a copy of the Registers, updated by the Service Provider up to the date of delivery of such Registers;

4.1.3 an inventory of Purchaser Data in the Service Provider 's possession or control;

4.1.4 details of any key terms of any third party contracts and licenses, particularly as regards charges, termination, assignation and novation;

4.1.5 a list of on-going and/or threatened disputes in relation to the provision of the Services;

4.1.6 all information relating to transferring Service Provider's Representatives required to be provided by the Service Provider under this Contract; and

4.1.7 such other material and information as the Purchaser shall reasonably require,

(together, the "**Exit Information**").

4.2 The Service Provider acknowledges that the Purchaser may disclose the Service Provider Sensitive Information (or any other information, whether confidential or otherwise) to an actual or prospective Replacement Service Provider or any third party whom the Purchaser is considering engaging to the extent that such disclosure is necessary in connection with such engagement (except that the Purchaser may not under this paragraph 4.2 of this Schedule disclose any such information where and to the extent that it relates to the Service Provider's or its Sub-Contractors' prices or costs).

4.3 The Service Provider shall:

4.3.1 notify the Purchaser within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Services and shall consult with the Purchaser regarding such proposed material changes; and

4.3.2 provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and in any event within ten (10) Working Days of a request in writing from the Purchaser.

4.4 The Service Provider may charge the Purchaser for its reasonable additional costs to the extent the Purchaser requests more than four (4) updates in any six (6) month period.

4.5 The Exit Information shall be accurate and complete in all material respects and the level of detail to be provided by the Service Provider shall be such as would be reasonably necessary to enable a third party to:

4.5.1 prepare an informed offer for those Services; and

4.5.2 not be disadvantaged in any subsequent procurement process compared to the Service Provider (if the Service Provider is invited to participate).

5. **EXIT PLAN**

5.1 The Service Provider shall, within three (3) months after the Effective Date, deliver to the Purchaser an Exit Plan which:

5.1.1 sets out the Service Provider 's proposed methodology for achieving an orderly transition of the Services from the Service Provider to the Purchaser and/or its Replacement Service Provider on the expiry or termination of this Contract;

5.1.2 complies with the requirements set out in paragraph 5.3 of this Schedule;

5.1.3 is otherwise reasonably satisfactory to the Purchaser.

5.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of its submission, then such dispute shall be resolved in accordance with the Management Arrangements.

5.3 Unless otherwise specified by the Purchaser, the Exit Plan shall set out, as a minimum:

5.3.1 how the Exit Information is obtained;

5.3.2 the management structure to be employed during both transfer and cessation of the Services;

5.3.3 the management structure to be employed during the Termination Assistance Period;

5.3.4 a detailed description of both the transfer and cessation processes, including a timetable;

5.3.5 how the Services will transfer to the Replacement Service Provider and/or the Purchaser, including details of the processes, documentation, data transfer, systems migration, security and the segregation of the Purchaser's technology components from any technology components operated by the Service Provider or its Sub-Contractors (where applicable);

5.3.6 details of contracts (if any) which will be available for transfer to the Purchaser and/or the Replacement Service Provider together with any reasonable costs required to effect such transfer (and the Service Provider agrees that all assets and contracts used by the Service Provider in connection with the provision of the Services will be available for such transfer);

5.3.7 proposals for the training of key individuals of the Replacement Service Provider's personnel in connection with the continuation of the provision of the Services charged at rates agreed between the Parties (each acting reasonably) at that time;

5.3.8 proposals for providing the Purchaser or a Replacement Service Provider copies of all documentation:

(a) used in the provision of the Services and necessarily required for the continued use thereof, in which the Intellectual Property Rights are owned by the Service Provider; and

(b) relating to the use and operation of the Services;

5.3.9 proposals for the assignation or novation of the provision of all services, leases, maintenance agreements and support agreements utilised by the Service Provider in connection with the performance of the supply of the Services to the extent required by the Purchaser or any Replacement Service Provider;

5.3.10 proposals for the identification and return of all Purchaser property in the possession of and/or control of the Service Provider or any third party (including any Sub-Contractor);

5.3.11 proposals for the disposal of any redundant Services and materials;

5.3.12 procedures to deal with requests made by the Purchaser and/or a Replacement Service Provider for information in respect of any Service Provider Representatives;

5.3.13 how each of the issues set out in this Schedule will be addressed to facilitate the transition of the Services from the Service Provider to the Replacement Service Provider and/or the Purchaser with the aim of ensuring that there is no disruption to or degradation of the Services during the Termination Assistance Period; and

5.3.14 proposals for the supply of any other information or assistance reasonably required by the Purchaser or a Replacement Service Provider in order to effect an orderly handover of the provision of the Services.

5.4 The Service Provider shall throughout the Contract Period review, and maintain the Exit Plan. If the Service Provider believes that any updates are required to the Exit Plan it shall provide written notification to the Purchaser outlining the details of any proposed updates. The Parties shall use reasonable endeavours to agree the contents of any updates to the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of its submission, then such dispute shall be resolved in accordance with the Management Procedures.

6. **TERMINATION ASSISTANCE**

6.1 The Purchaser shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Service Provider (a "**Termination Assistance Notice**") at any time prior to the end of the contract following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

6.1.1 the date from which Termination Assistance is required;

6.1.2 the nature of the Termination Assistance required; and

6.1.3 the period during which it is anticipated that Termination Assistance will be required ("**Termination Assistance Period**"), which shall continue no longer than twelve (12) months after the date that the Service Provider ceases to provide the Services.

6.2 The Purchaser shall have an option to extend the Termination Assistance Period beyond the period specified in the Termination Assistance Notice provided that such extension shall not extend for more than six (6) months beyond the end of the Termination Assistance Period and provided that it shall notify the Service Provider to such effect no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Purchaser shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Service Provider to such effect.

7. **TERMINATION ASSISTANCE PERIOD**

7.1 Throughout the Termination Assistance Period, or such shorter period as the Purchaser may require, the Service Provider shall:

7.1.1 continue to provide the Services and, if required by the Purchaser pursuant to paragraph 6.1 of this Schedule, provide the Termination Assistance;

7.1.2 in addition to providing the Services and the Termination Assistance, provide to the Purchaser any reasonable assistance requested by the Purchaser to allow the Services to continue without interruption following the termination or expiry of this Contract and to facilitate the orderly transfer of responsibility for and conduct of the Services to the Purchaser and/or its Replacement Service Provider;

7.1.3 use all reasonable endeavours to reallocate resources to provide such assistance as is referred to in paragraph 7.1.2 of this Schedule without additional costs to the Purchaser;

7.1.4 provide the Services and the Termination Assistance at no detriment to the Service Levels , save to the extent that the Parties agree otherwise in accordance with paragraph 7.3; and

7.1.5 at the Purchaser's request and on reasonable notice, deliver up-to-date Registers to the Purchaser.

7.2 Without prejudice to the Service Provider's obligations under paragraph 7.1.3 of this Schedule, if it is not possible for the Service Provider to reallocate resources to provide such assistance as is referred to in paragraph 7.1.2 of this Schedule without additional costs to the Purchaser, any additional costs incurred by the Service Provider in providing such reasonable assistance which is not already in the scope of the Termination Assistance or the Exit Plan shall be subject to the Change Control Procedure.

7.3 If the Service Provider demonstrates to the Purchaser's reasonable satisfaction that transition of the Services and provision of the Termination Assistance during the Termination Assistance Period will have a material, unavoidable adverse effect on the Service Provider 's ability to meet one or more particular Service Levels , the Parties (each acting reasonably) shall discuss and endeavour to agree a variation to the relevant Service Level(s) to take account of such adverse effect.

8. **TERMINATION OBLIGATIONS**

8.1 The Service Provider shall comply with all of its obligations contained in the Exit Plan.

8.2 Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Service Provider 's performance of the

Services and the Termination Assistance and its compliance with the other provisions of this Schedule), the Service Provider shall:

8.2.1 cease to use the Purchaser Data;

8.2.2 provide the Purchaser and/or the Replacement Service Provider with a complete and uncorrupted version of the Purchaser Data in (an open) electronic form (or such other format as reasonably required by the Purchaser);

8.2.3 erase from any computers, storage devices and storage media that are to be retained by the Service Provider after the end of the Termination Assistance Period all Purchaser Data and promptly certify to the Purchaser that it has completed such deletion;

8.2.4 return to the Purchaser such of the following as is in the Service Provider 's possession or control:

(a) all copies of the Purchaser Software and any other software licensed by the Purchaser to the Service Provider under this Contract;

(b) all materials created by the Service Provider under this Contract in which the Intellectual Property Rights are owned by the Purchaser;

(c) any items that have been on-charged to the Purchaser, such as consumables; and

(d) all Purchaser Property issued to the Service Provider. Such Purchaser Property shall be handed back to the Purchaser in good working order (allowance shall be made only for reasonable wear and tear);

(e) any sums prepaid by the Purchaser in respect of Services not delivered by the Expiry Date;

8.2.5 provide access during normal working hours to the Purchaser and/or the Replacement Service Provider for up to twelve (12) months after expiry or termination to:

(a) such information relating to the Services as remains in the possession or control of the Service Provider; and

(b) such members of the Service Provider Representatives as have been involved in the design, development and provision of the Services and who are still employed by the Service Provider, provided that the Purchaser and/or the Replacement Service Provider shall pay the reasonable costs of the Service Provider actually incurred in responding to requests for access under this paragraph.

8.3 Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Service Provider 's performance of the Services and the Termination Assistance and its compliance with the other provisions of this Schedule), each Party shall return to the other Party (or if requested, destroy or delete) all confidential information of the other Party (including the Purchaser Protected Information and the Service Provider Sensitive Information) and shall certify that it does not retain such information save to the extent (and for the limited period) that such information needs to be retained by the Party in question for the purposes of providing or receiving any Services or termination services or for statutory compliance purposes.

8.4 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Purchaser to the Service Provider in relation to the Services shall be terminated with effect from the end of the Termination Assistance Period.

9. **ASSETS, SUB-CONTRACTS AND SOFTWARE**

9.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Service Provider shall not, without the Purchaser's prior written consent:

9.1.1 terminate, enter into or vary any Sub-Contract;

9.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Service Provider Assets or acquire any new Service Provider Assets; or

9.1.3 terminate, enter into or vary any license for software in connection with the provision of Services.

9.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Service Provider pursuant to paragraph 7.1.5 of this Schedule, the Purchaser shall provide written notice to the Service Provider setting out:

9.2.1 which, if any, of the Transferable Assets the Purchaser requires to be transferred to the Purchaser and/or the Replacement Service Provider ("**Transferring Assets**");

9.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Purchaser and/or the Replacement Service Provider requires the continued use of; and

9.2.3 which, if any, of Transferable Contracts the Purchaser requires to be assigned or novated to the Purchaser and/or the Replacement Service Provider (the "**Transferring Contracts**"), in order for the Purchaser and/or its Replacement Service Provider to provide the Services from the expiry of the Termination Assistance Period. Where requested by the Purchaser and/or its Replacement Service Provider, the Service Provider shall provide all reasonable assistance to the Purchaser and/or its Replacement Service Provider to enable it to determine which Transferable Assets and Transferable Contracts the Purchaser and/or its Replacement Service Provider requires to provide the Services.

9.3 With effect from the expiry of the Termination Assistance Period, the Service Provider shall sell the Transferring Assets to the Purchaser and/or its nominated Replacement Service Provider for a consideration equal to their Net Book Value, except where the cost of the Transferring Asset has been partially or fully paid for through the Contract Charges at the end of contract, in which case the Purchaser shall pay the Service Provider the Net Book Value of the Transferring Asset less the amount already paid through the Contract Charges.

9.4 Risk in the Transferring Assets shall pass to the Purchaser or the Replacement Service Provider (as appropriate) at the end of the Termination Assistance Period and title to the Transferring Assets shall pass to the Purchaser or the Replacement Service Provider (as appropriate) on payment for the same.

9.5 Where the Service Provider is notified in accordance with paragraph 9.2.2 of this Schedule that the Purchaser and/or the Replacement Service Provider requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Service Provider shall as soon as reasonably practicable:

9.5.1 procure a non-exclusive, perpetual, royalty-free license (or license on such other terms that have been agreed by the Purchaser) for the Purchaser and/or the Replacement Service Provider to use such assets (with a right of sub-license or assign on the same terms); or

9.5.2 failing which procure a suitable alternative to such assets and the Purchaser or the Replacement Service Provider shall bear the reasonable proven costs of procuring the same.

9.6 The Service Provider shall as soon as reasonably practicable assign or procure the novation to the Purchaser and/or the Replacement Service Provider of the Transferring Contracts. The Service Provider shall execute such documents and provide such other assistance as the Purchaser reasonably requires to effect this novation or assignation.

9.7 The Purchaser shall:

9.7.1 accept assignations from the Service Provider or join with the Service Provider in procuring a novation of each Transferring Contract; and

9.7.2 once a Transferring Contract is novated or assigned to the Purchaser and/or the Replacement Service Provider, carry out, perform and discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Service Provider does the same.

9.8 The Service Provider shall hold any Transferring Contracts on trust for the Purchaser until such time as the transfer of the relevant Transferring Contract to the Purchaser and/or the Replacement Service Provider has been effected.

9.9 The Service Provider shall indemnify the Purchaser (and/or the Replacement Service Provider, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Purchaser (and/or Replacement Service Provider) pursuant to paragraph 9.6 of this Schedule in relation to any matters arising prior to the date of assignation or novation of such Transferring Contract.

10. **SERVICE PROVIDER PERSONNEL**

10.1 The Service Provider shall not take any step (expressly or implicitly and directly or indirectly by itself or through any other person) to dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Purchaser and/or the Replacement Service Provider.

10.2 During the Termination Assistance Period, the Service Provider shall give the Purchaser and/or the Replacement Service Provider reasonable access to the Service Provider 's personnel to present the case for transferring their employment to the Purchaser and/or the Replacement Service Provider.

10.3 The Service Provider shall immediately notify the Purchaser or, at the direction of the Purchaser, the Replacement Service Provider of any period of notice given by the Service Provider or received from any person referred to in the information to be provided by the Service Provider pursuant to Section D (staff involved in the provision of services) of the Contract, regardless of when such notice takes effect.

10.4 The Service Provider shall not for a period of twelve (12) months from the date of transfer actively seek to re-employ or re-engage or entice any employees, or Sub-Contarctors whose employment or engagement is transferred to the Purchaser and/or the Replacement Service Provider.

11. **CHARGES**

11.1 Except as otherwise expressly specified in this Contract, the Service Provider shall not make any charges for the services provided by the Service Provider pursuant to, and the Purchaser shall not be obliged to pay for costs incurred by the Service Provider in relation to its compliance with, this Schedule including the preparation and implementation of the Exit Plan, the Termination Assistance and any activities mutually agreed between the Parties to carry on after the expiry of the Termination Assistance Period.

12. **APPORTIONMENTS**

12.1 All outgoings and expenses (including any remuneration due) and all rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Purchaser and the Service Provider and/or the Replacement Service Provider and the Service Provider (as applicable) as follows:

12.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

12.1.2 the Purchaser shall be responsible for (or shall procure that the Replacement Service Provider shall be responsible for) or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

12.1.3 the Service Provider shall be responsible for or entitled to (as the case may be) the rest of the invoice.

12.2 Each Party shall pay (and/or the Purchaser shall procure that the Replacement Service Provider shall pay) any monies due under paragraph 12.1 of this Schedule as soon as reasonably practicable.

This and the following single page comprise Schedule 11 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 11 - BUSINESS CONTINUITY AND DISASTER RECOVERY

1. SERVICE PROVIDER'S BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

The Service Providers Business Continuity and Disaster Recovery plan will be inserted following contract award.

This and the following 4 pages comprise Schedule 12 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 12 - SECURITY

DEFINITIONS

1.1 In this Schedule 12, the following definitions shall apply:

"**Breach of Security**" means the occurrence of:

(a) any unauthorised access to or use of the Services, the Sites, the Service Provider System and/or any ICT, information or data (including the Purchaser Protected Information, the Service Provider Sensitive Information, the Purchaser Data, and Customer personal data) used by the Purchaser and/or the Service Provider in connection with the Contract; and/or

(b) the loss and/or unauthorised disclosure of any information or data (including the Purchaser Protected Information, the Service Provider Sensitive Information, the Purchaser Data, and Customer personal data), including any copies of such information or data, used by the Purchaser and/or the Service Provider in connection with the Contract, in either case as more particularly set out in the Security requirements in this Schedule 12 and any relevant Security Policy;

(c) an unauthorised change to the integrity or accuracy of the information or data being processed.

2. **SECURITY MANAGEMENT PLAN**

2.1. Within twenty (20) Working Days after the Effective Date, the Service Provider shall prepare and submit to the Purchaser for Approval in accordance with paragraph 2 of this Schedule a fully developed, complete and up-to-date Security Management plan which shall comply with the requirements of paragraph 2.2 of this Schedule (the "**Security Management Plan**").

2.2. The Security Management Plan shall:

2.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan) to this Schedule 12;

2.2.2 comply with the relevant security policies, and/or any security measures specified in Schedule 9 (Model Contract regarding Data Protection Directive 95/46/EC), and any other security policies and/or security measure notified to the Service Provider;

2.2.3 unless otherwise specified by the Purchaser in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Purchaser's premises, the Sites, the Service Provider System and any ICT, information and data (including the Purchaser Protected Information, the Service Provider Sensitive Information, the Purchaser Data, and Customer personal data) to the extent used by the Purchaser or the Service Provider in connection with the Contract;

2.2.4 set out the security measures to be implemented and maintained by the Service Provider in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule 12.

2.2.5 set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those set out in the Implementation Plan for the Service Provider to meet the full obligations of the security requirements set out in Schedule Annex 1 (Security) to this Schedule 12.

2.2.6 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

2.2.7 be written in plain English in language which is readily comprehensible to the staff of the Service Provider and the Purchaser engaged in the Services and shall reference only documents which are in the possession of the Purchaser or whose location is otherwise specified in this Schedule 12.

2.3. If the Security Management Plan submitted to the Purchaser pursuant to paragraph 2.1 of this Schedule is Approved by the Purchaser, it shall be adopted by the Service Provider immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Purchaser, the Service Provider shall amend it within ten (10) Working Days of a notice of non-approval from the Purchaser and re-submit it to the Purchaser for Approval. The Parties shall use all reasonable endeavours to ensure that the Purchaser process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of the first submission to the Purchaser of the Security Management Plan. If the Purchaser does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Management Arrangements. No Approval to be given by the Purchaser pursuant to this paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in paragraph 2.2 of this Schedule shall be deemed to be reasonable.

2.4. Approval by the Purchaser of the Security Management Plan pursuant to paragraph 2.3 of this Schedule or of any change or amendment to the Security Management Plan shall not relieve the Service Provider of its obligations under this Schedule or the Contract.

3. **AMENDMENT AND REVISION OF THE SECURITY MANAGEMENT PLAN**

3.1. The Security Management Plan shall be fully reviewed and updated by the Service Provider from time to time and at least annually to reflect:

3.1.1. emerging changes in Good Industry Practice;

3.1.2. any change or proposed change to the Service Provider System, the Services and/or associated processes;

3.1.3. any new perceived or changed security threats; and

3.1.4. any reasonable request by the Purchaser.

3.2. The Service Provider shall provide the Purchaser with the results of such reviews as soon as reasonably practicable after their completion and the Security Management Plan at no additional cost to the Purchaser. The results of the review shall include, without limitation:

3.2.1. suggested improvements to the effectiveness;

3.2.2. updates to the risk assessments;

3.2.3. proposed modifications to the procedures and controls that effect information security to respond to events; and

3.2.4. suggested improvements in measuring the effectiveness of controls.

3.3. Subject to paragraph 3.4 of this Schedule, any change or amendment which the Service Provider proposes to make to the Security Management Plan (as a result of a review carried out pursuant to paragraph 3.1 of this Schedule, a Purchaser request, change to Annex 1

(Security) to this Schedule 12 or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until Approved in writing by the Purchaser.

3.4. The Purchaser may, where it is reasonable to do so, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to such procedures for the purposes of formalising and documenting the relevant change or amendment for the purposes of the Contract.

4. **BREACH OF SECURITY**

4.1. Either Party shall notify the other in accordance with the agreed security incident management process as defined by the Security Management Plan upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

4.2. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 4.1 of this Schedule, the Service Provider shall:

4.2.1 immediately take all steps (which shall include any action or changes required by the Purchaser) necessary to:

(a) remedy such Breach of Security or any potential or attempted Breach of Security or protect the integrity of the Security Management Plan against any such Breach of Security or any potential or attempted Breach of Security; and

(b) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

4.2.2 promptly provide to the Purchaser full details of the Breach of Security or the potential or attempted Breach of Security, including a root cause analysis where required by the Purchaser.

4.3. In the event that such action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance with any security policies notified to the Service Provider, the terms of the Security Management Plan, or security requirements or other requirements set out in the Contract (including this Schedule), or is otherwise due to the Default of the Service Provider, then any required change to the Security Management Plan shall be at no cost to the Authority.

5. PENETRATION TEST OF RELATED SYSTEMS

5.1. The Service Provider shall ensure that the Service Provider System is tested on at least an annual basis by an accredited tester and that vulnerabilities are actioned in line with recommended actions.

5.2. The Service Provider shall ensure that an accredited penetration test specific to the hosted website(s) is conducted: (i) on at least an annual basis; and (ii) promptly at any time during the Contract Period should significant changes be implemented that have the possibility of introducing weaknesses to those systems.

5.3. The Service Provider shall ensure that any recommended actions coming out of any testing outlined in paragraphs 5.1 and 5.2 are implemented promptly to remove or mitigate any discovered vulnerabilities.

5.4. The Service Provider will ensure that all checks and testing are aligned with business objectives (i.e. scope, constraints, deliverables) and that remedial actions are actioned promptly in line with business requirements.

ANNEX 1: SECURITY REQUIREMENTS

[NOTE: SECURITY REQUIREMENTS TO BE INSERTED FOLLOWING CONTRACT AWARD DEPENDING ON DATA TRANSFER REQUIREMENTS AND DETAILS BEING FINALISED.]

ANNEX 2: SECURITY MANAGEMENT PLAN

A Security Plan shall be provided by Service Provider within 20 working days of Contract Award.

This and the following single page comprise Schedule 13 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 13 - IMPLEMENTATION PLAN

1. SERVICE PROVIDER'S IMPLEMENTATION PLAN

An Implementation Plan to be provided by Service Provider within 10 Working Days of Contract Award.

SOCOTEC
CERTIFICATION
INTERNATIONAL

CERTIFICATE

N° 13487IS

certifies that:

PeoplePlus

Blades Enterprise Centre John Street Sheffield S2 4WS

operates a management system that has been assessed as conforming to:

ISO/IEC 27001 : 2013

for the scope of activities:

The Information Security for job search support, work placement and one-to-one mentoring and training across employability and skills provision in accordance with the Statement of Applicability 2.1, 29/07/15

Issue date: **20 January 2017**
Valid until: **13 January 2018** (Subject to adherence to the agreed ongoing programme, successful endorsement of certification following each audit and compliance with the terms and conditions of certification.)
Original date of certification: **20 September 2012**

Emma Law Operations Director

UKAS MANAGEMENT SYSTEMS
0063

SOCOTEC Certification UK Delta Business Park -
Swindon SN5 7XP - UNITED KINGDOM
www.socotec-certification-international.com

UK-00000000001

CGI-23022017-EN-UK

Document Retention Policy

Policy Owner	Review Date
Head of Assurance	June 2017

This Policy is the work of PeoplePlus and the Copyright in such is vested with PeoplePlus and should not be re-worked, modified or copied for use by any individual without the formal, written agreement of PeoplePlus. This Policy and the detail set out herein represents confidential information of PeoplePlus and should not be disclosed beyond the intended recipient without the express, written agreement of a duly authorised representative of PeoplePlus. Should you have any doubt as to whether this document should be disclosed to any party, please contact the Contracts Support Team who will provide you with advice and guidance. Any breach by any individual of Copyright or confidentiality will be considered by PeoplePlus to be a breach of contract in relation to any employee, subcontractor or consultant to PeoplePlus and will be dealt with under the remedies within those agreements.

jobcentreplus
Department for Work and Pensions

Funded by
Skills Funding Agency

European Union
European Social Fund

© Copyright PeoplePlus. 2015 Commercial in Confidence

1.0 Introduction

1.1 The Company recognises the importance of effective controls in the management of documents, records and electronic data which includes a comprehensive retention policy that meets legislative and contract requirements.

2.0 Scope

2.1 This Policy relates to the identification, storage, protection, retention, retrieval, and disposal of all documents and records relating to the Company's operation of contracted employment provision and more specifically to the following documentation identified in the relevant Supplier Guidance:

a) Sustainable Development Action Plans;
b) Equality and Diversity Action Plans;
c) Publicity evidence (sample documents containing ESF logo);
d) Customer Action Plans;
e) Attendance register/timesheet;
f) Training Allowance forms;
g) Travel and subsistence costs (evidence of amounts paid and supporting documentation for claims for Match contracts only);
h) Childcare costs (evidence of amounts paid and supporting documentation for claims for Match contracts only);
i) Additional Support (evidence of amounts paid and supporting documentation for claims for Match contracts only);
j) Supporting evidence of job outcomes;
k) Supporting evidence of qualification outcomes; and
l) Soft outcome evidence.

© Copyright PeoplePlus. 2015 Commercial in Confidence

2.2 Except where specifically referred to in this Policy, the identification, storage, protection, retention, retrieval, and disposal of electronic data shall be subject to the controls detailed in the following Company documents:

a) Security Plan
b) Information Security Policy

3.0 Responsibilities

3.1 It is the responsibility of the Head of Assurance to initiate this Policy and ensure that it is reviewed periodically. The Head of Assurance shall also ensure that procedures covering document retention and control are subject to scheduled internal quality audits.

3.2 It is the responsibility of the IT Director to ensure that policies and procedures relating to the storage, retention and retrieval of electronic data (including customer information) are in place and reviewed regularly.

3.3 It is the responsibility of delivery centre managers (including subcontractors) to ensure that policy and procedures relating to document retention are carried out at their respective sites.

3.4 It is the responsibility of all staff to ensure that they comply with directives on documents storage, retention and retrieval with their areas.

4.0 Policy Statement

4.1 To comply with the principles of the Data Protection Act, records containing personal data must be:

a) Stored appropriately with due regard to the sensitivity and confidentiality of the information recorded and with the prevention of access by unauthorised persons;

© Copyright PeoplePlus. 2015 Commercial in Confidence

b) Retrievable and easily traced;

c) Retained for as long as is necessary in accordance with statutory and requirements; and

d) Disposed of appropriately after statutory and contractual retention periods have elapsed to prevent access by unauthorised persons.

5.0 Identification

5.1 All documents and records shall have an appropriate unique identifier or reference number that allows easy identification and retrieval.

5.2 Customer records shall be indexed and stored alphabetically both whilst active (e.g. in current use) and when archived (e.g. no longer in current use).

5.3 Customer records shall be archived in boxes labelled with a unique identifier, relative to the contract name and start date as specified by DWP or other funding body. All customer records (mapped by the unique Customer ID number) will be catalogued against each uniquely identified archive box.

6.0 Storage, Protection and Retrieval

6.1 All documents, records and electronic data shall be stored as securely as possible in order to prevent potential misuse or loss.

6.2 Company staff must refer to the current version of the following Company Policy with regard to the organisation's commitments and responsibilities for backing up information assets:

a) Information Security Policy.

6.3 All documents, records and data shall be stored in the most secure and appropriate location to facilitate easy access and retrieval. These locations will be on the Company's premises until such time that records, due to volume,

© Copyright PeoplePlus. 2015 Commercial in Confidence

age or the fact that they are no longer active, need to be removed and stored at a secure external site.

6.4 The Company shall only use Department for Work and Pensions (DWP) approved organisations for the storage of documents and records at external sites.

6.5 All documents and records that contain personal information in any form shall be considered as confidential in nature and shall be protected accordingly.

6.6 All documents and records shall be stored both within Company premises and at DWP approved external storage depots in such a manner to facilitate easy retrieval in the event of internal or external audit and/or investigation.

7.0 Retention

7.1 The Company shall not retain documents and records longer than is necessary and in accordance with the Data Protection Act 1998 personal data processed for any purpose shall not be kept for longer than is necessary for that purpose.

7.2 However, ESF audit regulations and contractual obligations require the documents and records listed above to be retained until at least 31st December 2022, or 31st December 2030 (refer to the specific contract requirements for confirmation) and the Company shall comply with these regulations.

7.3 In accordance with DWP Supplier Guidance, documents and records (for example – job outcome supporting evidence) may be retained as electronic copy of the original but must meet with Commission Regulation (EC) 2355/2002 and:

a) Be held on a recognised data carrier;

© Copyright PeoplePlus. 2015 Commercial in Confidence

b) Be certified as copies of the original;

c) Be able to be audited.

7.4 Such electronic copies shall include the DWP or other funding body (as appropriate) approved wording to declare that the Company is certifying that the document is a true copy of the original.

7.5 Signatures on declarations certifying that the electronic document is a true copy of the original shall be original signatures.

8.0 Destruction and Disposal

8.1 Company staff must refer to the current version of the following policy with regard to the secure disposal of all printed materials and removable storage media:

a) Information Security Policy – 6.3 (Disposal and Decommissioning)

© Copyright PeoplePlus. 2015 Commercial in Confidence

PeoplePlus

Information Security Policy

Version 1.2

16.02.2017

Document Control

Date	Version	Comments
23/11/2015	1.1	Final draft approved by Information Security Forum
16/02/2017	1.2	Final draft approved by Information Security Forum

Contents

1. Foreword 6

1.1 Security Goals 6

1.2 Scope of Coverage 6

2. Roles & Responsibilities 8

2.1 Owner of the Security Policy 8

2.2 Head of Assurance 8

2.3 System Owners 8

2.4 System Administrator 8

2.5 Users 8

2.6 Contractual Partners 8

3. Human Resources 9

3.1 Human Resources Security Policy 9

3.1.1 Prior to employment 9

3.1.2 During employment 11

3.2 Mobile Phone Usage Policy 13

3.3 Email Usage Policy 14

3.3.1 Personal Use 14

3.3.2 Instant Messaging 14

3.3.3 Web mail accounts 14

3.4 Internet Usage Policy 17

3.4.1 Personal Use 18

3.4.2 Monitoring 20

4 Information Asset Management 21

4.1 IT Asset Management Policy 21

4.1.1 Acquisition and Procurement of IT Assets 21

4.1.2. Asset tagging and recording 21

4.1.3 Software Asset Management (SAM 21

4.1.4 Operational Management of IT Assets 21

4.1.6 Inactive assets 22

4.1.7 In-lifecycle changes 22

4.1.8 Lost and Stolen Assets 22

4.1.9 Recovery of assets from staff leaving the company 23

4.1.10 Asset Disposal 23

4.2 Information Classification & Handling Policy 24
4.2.1 Information Classifications 25
4.2.2 Information Handling Rules 27
5 Access Control 30
5.1 Access Control Policy 30
5.2 User ID & Password Policy 31
5.3 Remote Access Security Policy 33
6 Cryptography 34
6.1 Encryption Security Policy 34
7 Physical and Environmental Security 36
7.1 Physical Security Policy 36
7.1.1 Storage of sensitive assets 36
7.1.2 Office areas 37
7.1.3 Building security 37
7.1.4 Physical access control 37
7.1.5 Incoming and Outgoing mail and deliveries 37
7.1.6 Manned guarding 38
7.1.7 CCTV 38
7.1.8 Intruder Alarms 38
7.1.9 Photography, Audio and/or Video Recording 38
7.2 Equipment Security Policy 39
7.3 Disposal and Decommissioning Security Policy 40
7.4 Clear Desk and Screen Security Policy 42
8 Operations Security 44
8.1 Change Control Policy 44
8.2 Security Monitoring Policy 44
8.3 Anti-Malware Security Policy 45
8.4 Logging and Monitoring Security Policy 46
8.5 PCs, Tablets and Laptop Security Policy 47
8.6 Authentication Security Policy 49
8.6.1 Web Authentication 49
8.6.2 Voice Authentication 49
8.6.3 Email Authentication 49
9 Communications Security 50

9.1 Network Security Policy 50
9.2 Firewall Security Policy 51
9.3 Router and Switch Security Policy 52
9.4 Wireless Security Policy 53
9.5 External Communications Security Policy 54
9.5.1 Public and semi-public places 54
9.5.2 Talking to people outside the company 55
9.5.3 Contact from a journalist, MP or other official 55
9.5.4 Reporting potential media coverage 55
9.5.5 Management of all external communications/materials 55
9.5.6 Websites and Online Technologies 56
9.5.7 Partners, Subcontractors and Suppliers 56
10 System Acquisition Development and Maintenance 57
10.1 Database Security Policy 57
10.1.1 Database Development & Design 57
10.1.2 Database Use & Operation 58
11 Supplier Relationships 60
11.1 Third Party Security Policy 60
12 Information security incident management 62
12.1 Incident Response Security Policy 62
12.1.1 Security Incidents 62
12.1.2 Investigations and evidence 63
13 Information Security Aspects of Business Continuity 65
13.1 Business Continuity Security Policy 65
14 Compliance Security Policies 66
14.1 Compliance Security Policy 66
14.2 Records Management Policy 68
15 Other Policies 70
15.1 Remote/Mobile Computing Policy 70
15.2 Data Protection, Copyright & Confidentiality Policy 73

1. Foreword

PeoplePlus is committed to safeguarding the confidentiality, integrity and availability all information assets. The purpose of this policy is to identify, assess, and appropriately mitigate vulnerabilities and threats to PeoplePlus which through the loss, corruption or unauthorised access to critical information could adversely impact the critical business assets of the organisation. This includes ensuring business continuity and minimising business damage by preventing, detecting and responding to information security incidents and managing information security risks.

1.1 Security Goals

The overall aim for this Policy is to ensure that:

- Confidentiality of PeoplePlus information assets is maintained.
- Integrity and authenticity of information is maintained.
- Availability and usability of information is maintained.
- Information is protected against unauthorised access.
- Authentication is appropriately applied to validate user identities.
- Contractual, Regulatory and Legislative Information Security requirements are met.
- Business Continuity and risk management plans are produced, maintained and tested.
- Change management is applied to maintain security.
- Information security awareness training is available to all staff.
- All security breaches, actual or suspected, are reported and investigated and action taken to improve procedures where required.
- Information Security Policies, Procedures and Guidelines are documented and implemented to support this policy.
- All information assets will be subject to formal risk assessment and treatment.
- The Security Policy and the supporting policy documents are reviewed at least every six months by the Information Security Forum.
- To ensure that learners, customers and staff are protected from the risk of radicalisation and extremism when using our IT systems

The Senior Management of PeoplePlus approves this policy.

1.2 Scope of Coverage

This Policy applies to all PeoplePlus operations, supported ICT and operational infrastructure, information assets, information systems and security management processes. It applies to all directors, users and stakeholders of the organisation.

The above definition of user includes all individuals who have been authorised to use PeoplePlus systems and services in line with the Access Control Policy in Section 4 of this policy.

2. Roles & Responsibilities

2.1 Owner of the Security Policy

The Managing Director is responsible for the maintenance, review and implementation of this policy and all its supporting policies under this Policy.

2.2 Head of Assurance

The Managing Director delegates the implementation and maintenance responsibility information security to the Head of Assurance working through the Information Security Forum which comprises the Head of Assurance and representatives from the key business functions. The Information Security Forum will implement the Information Security Policy throughout PeoplePlus. The Head of Assurance has direct responsibility for maintaining the Information Security Policy framework while providing advice and guidance with the support of the Information Security Forum.

2.3 System Owners

All systems will be assigned a system owner. The system owner, in consultation with the IT department, is responsible for purchasing requirements, development and maintenance of information and related information systems. All systems and all types of information must have a defined owner. The system owner must define which users or user groups are allowed access to the information and what authorised use of this information consists of.

2.4 System Administrator

All systems will be assigned a system administrator. System administrators are persons administrating PeoplePlus information systems and the information entrusted to the company by other parties. Each type of information and system may have one or more dedicated system administrators. These are responsible for protecting the information, including implementing systems for access control to safeguard confidentiality, and carry out backup procedures to ensure that critical information is not lost. They will further implement, run and maintain the security systems in accordance with the security policy. Each system must have one or more system administrators.

2.5 Users

All users are responsible for complying with the Information Security Policy and any associated procedures and regulations.

2.6 Contractual Partners

Contractual partners and contracted consultants are bound by all the provisions contained within the policy and must sign a confidentiality agreement prior to accessing sensitive information. The System Owner is responsible for ensuring that this is implemented.

3. Human Resources

3.1 Human Resources Security Policy

The Human Resources Security Policy details the security requirements prior to, during and post-employment.

3.1.1 Prior to employment

PeoplePlus will ensure that employees, contractors and third party users understand their information security responsibilities, and are suitable for the roles they are considered for to reduce the risk of fraud, misuse of the facilities or theft of the organisation's property. Security responsibilities should be addressed prior to employment in job descriptions and terms and conditions of employment. All candidates for employment should be screened in relation to the sensitivity of the role they are being considered for. All employees should sign an IT User agreement detailing their responsibilities relating to the use of information and associated processing facilities.

3.1.1.2 Roles and responsibilities

Security Roles and responsibilities are documented jointly in 2 Roles and Roles Security Policy and the Organisation of Security. Security roles and responsibilities of employees, contractors and third party suppliers should be defined and documented according to this security policy. The relevant roles and responsibilities should be clearly communicated to job candidates during the pre-employment process. They should include the requirement to:

- Implement and act in accordance with the information security policies,
- Protect the organisation's assets from unauthorised access, disclosure, modification, destruction or interference,
- Carry out and comply with security processes and activities detailed within their job description,
- Ensure that responsibility is assigned to individuals for actions taken,
- Report actual or potential security events or risks to the information security team.

These requirements may be summarised in job descriptions supplied to agencies and potential candidates.

3.1.1.2 Personnel screening

Prior to completing an unconditional employment offer, PeoplePlus will carry out the background checks, including a combination of the following:

- Verifying references from previous employers.

- Confirmation of any academic or professional credentials claimed if compulsory for the role
- User identity check against passport or other approved documentation verifying an individual's right to work in the UK.
- DBS check for eligible roles

These checks are considered to comply with the cabinet office requirement for all employees to undergo Baseline Personal Security Standard (BPSS) checks as part of the pre-employment process. PeoplePlus may perform other checks for certain roles for which there is a specific contractual, regulatory or legal obligation. These checks can include credit or Security Clearance checks but will be directly related to the classification of the information to be accessed and the sensitivity of the role e.g. access to public funds and accounts. All personal information gathered in relation to individual job applications will be treated as sensitive and handled in accordance with the data protection act and the Data Classification and Handling Policy.

3.1.3 False or misleading credentials

An applicant who deliberately or knowingly provides misleading, erroneous, or deceptive information in an application form, CV, or during an interview may be immediately eliminated from any further consideration for employment.

Any subsequent revelation which indicates that an employee deliberately or knowingly provided incorrect information during the recruitment process may lead to dismissal and/or referral to external authorities.

3.1.4 Terms and conditions of employment

As part of their contractual obligation, employees, contractors and third party suppliers should agree and sign the terms and conditions of their employment. This should state both their and PeoplePlus's responsibilities for information security.

The security specific terms and conditions of employment should make direct reference to the security policies and state:

- That all employees, who are given access to sensitive information should sign a confidentiality and security statement or nondisclosure agreement prior to being given access to information processing facilities,
- The employees responsibilities in relation to relevant legislation i.e. data protection and freedom of information,
- The employees responsibilities to understand and comply with all organisational policies,
- Responsibilities for handling, management and protection of sensitive assets, in particular, personal data,
- Actions to be taken in the event that any employee disregards the organisation's security requirements.

The responsibility to maintain the confidentiality of PeoplePlus information stated within the terms and conditions of employment should continue beyond employment. The Terms and Conditions of employment will state that users' computers and

activities may be monitored to ensure compliance with the Information Security Policy.

3.1.2 During employment

Employees must be aware of information security threats, their responsibilities and liabilities and be able to support the security requirements of the organisation during their work to reduce the risk of human error.

3.1.2.1 Management responsibilities

PeoplePlus requires all employees to apply and adhere to information security in accordance with the relevant policies. This should ensure that all employees:

- Are properly briefed on their information security roles prior to being granted access to any sensitive information or resources,
- Are provided with guidelines which state the security expectations of their role,
- Are motivated to comply with the security policies,
- Achieve and maintain a level of security awareness relevant to their role,
- Comply with the terms and conditions of their employment including the security requirements.

3.1.2.2 Information security awareness and training

All PeoplePlus employees, and where relevant, contractors and third party suppliers, will receive security awareness training and regular updates on security policies and procedures as well as notification of any changes to applicable legislation and guidelines. The security and awareness training given to personnel will be relevant to individuals' roles, responsibilities and skills. It will include updates on current security issues and threats and will contain reminders on the need to report any incidents or risks to the information security team.

Employees will be given the opportunity to provide feedback on the relevance, content, and effectiveness of the information and training they receive.

3.1.2.3 New employees security briefing

All new employees, both permanent and contract must receive an initial security briefing within the first month of employment as part of an induction program. This briefing will ensure that they understand the implications of the security requirements, protection methods and controls used while performing their jobs. This includes the importance of security, the use of security measures, asset protection rules, acceptable use policy and the process of reporting any security violations.

3.1.2.4 Continuous education

All staff will be regularly reminded about their obligations in respect to information security. Security reminders will be provided to all users via the intranet and other appropriate communications; these will include 'hot' topics with the aim of maintaining a high level of security awareness throughout the organisation. Where

required, security courses and specifically targeted security training will be provided. These will ensure continued security education for all staff and cover at least the basic security requirements. Management are required to allocate sufficient on-the-job time for staff to familiarise themselves and remain current with security policies and procedures.

3.1.2.5 Disciplinary process

The HR disciplinary process will be applied to cases of employees committing a security breach. However, this will not commence prior to the verification that a security breach has occurred and will ensure that correct and fair treatment is applied. Where a serious security breach has been verified consideration will be given to the immediate revocation of employee access rights and privileges.

3.1.3 Termination or change of employment

The HR team has responsibility for the employment termination process and will work with the line manager of the employee leaving to ensure that all the relevant security aspects are applied to the process. The termination process for contractors or third party supplier staff will be handled by the responsible agency or direct employer. Contracts with employment agencies or third party suppliers will include the requirement to comply with this policy.

3.1.3.1 Return of assets

All employees are required to return all PeoplePlus assets on termination of employment, contract or agreement via their line manager, this includes:

- Hardware (laptops, PCs or smart phones)
- Media storage devices (USB drives, CDs or DVDs)
- Physical and logical access tokens (VPN tokens, door access swipe cards)
- PeoplePlus documents
- Software
- Manuals

Employees will be asked by their line manager to confirm that they no longer have any PeoplePlus assets in their possession prior to their final working day.

3.1.2.2 Removal of access rights

The access rights of all employees, contractors and third party users to information and information processing facilities will be removed on termination of employment, contract or agreement, or adjusted as necessary on change of role. This is detailed in the Access Control section of this document and should be carried out by their line manager.

This aspect is of particular importance where an employee is dismissed following a disciplinary process or suspended pending the outcome of an investigation. It should take account of both physical and logical access rights. Any shared team or

departmental access rights such as door codes or passwords to shared services should also be changed.

3.2 Mobile Phone Usage Policy

The Mobile Phone Usage Policy is intended to assist all those who use mobile phones for company business and to detail PeoplePlus's policy for the use of personal mobile phones during business hours.

Company mobile phones are the property of the PeoplePlus. As with all company equipment it is provided for business use.

It is the responsibility of individual members of staff to ensure the security of company mobile phones. This includes precautions such as never leaving the phone on display in a car, left unattended on a desk or lending the phone to anyone else to use. Staff must use a PIN number with the phone and never disclose this to anyone else. It is imperative that staff report any loss, damage or theft immediately to their line manager. In the event of loss, damage or theft of a phone, the company reserves the right to reclaim the cost associated in replacing the phone back from the individual. All phones which are stolen should be reported to the Police and a crime number obtained which will be required for insurance purposes. The Head of Assurance should also be informed of the theft as the theft could have Information Security implications.

The company accepts the fact that for many employees, the use of a mobile phone is part of their everyday work. It also recognises that prolonged use of mobile phones may cause health problems and suggests that mobile phone usage is restricted to a minimum. For safety reasons PeoplePlus staff must not use a handheld mobile phone whilst driving any vehicle. It is illegal to do so and staff must pull over at the earliest opportunity, when and where safe to do so and switch off the engine to make or return a call. PeoplePlus will not take responsibility or be liable in any way for someone charged with using a handheld device whilst driving. All hand held usage, whilst a vehicle is moving, is strictly prohibited and could involve disciplinary action being taken against any individual found to be in breach of this policy.

PeoplePlus recognises that many staff members have access to a hands free kit but recommends it is best not to use a hands free phone while driving. Using a hands free phone will distract you. For your own safety, and that of other road users avoid taking and making calls or using text messaging whilst driving. All company mobile phones should be left switched on during office hours but turned to silent mode during meetings.

3.3 Email Usage Policy

The purpose of this policy is to ensure the proper use of the PeoplePlus email system and make users aware of what PeoplePlus deems as acceptable and unacceptable use of its email system. PeoplePlus reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

3.3.1 Personal Use

Whilst PeoplePlus permits personal use of the email system, it should be noted that this is a privilege and not a right. Such use shall be kept to a minimum.

Unacceptable use of the email system includes, but is not limited to the following:

- Use of the PeoplePlus email system for business purposes other than that of PeoplePlus.
- Use of the PeoplePlus email system for storing or distributing images, text or materials that may be considered discriminatory, offensive, abusive, indecent, pornographic, obscene or illegal.
- Breaking into PeoplePlus's or another organization's system or unauthorized use of a password or mailbox
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters
- Transmitting unsolicited commercial or advertising material
- Undertaking deliberate activities that waste staff or systems resources
- Knowingly introducing any form of computer virus or malware into the corporate network
- Sending personal email containing PeoplePlus customer or commercially sensitive information with the aim of removing it from the business without permission.
- Use email to perpetrate any form of fraud or to breach any laws

Please note that although you have control over the password you use to gain access to PeoplePlus systems, this does not constitute an expectation of privacy. This should be taken into account when using PeoplePlus systems for personal correspondence. Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.

3.3.2 Instant Messaging

The use of Instant Messaging tools such as MSN Messenger and Yahoo Messenger for any communication is not permitted as such tools can introduce serious security vulnerabilities. SMS messaging is permitted for client communications.

3.3.3 Web mail accounts

Web mail accounts are email services which can be accessed via the Internet from

any location. The only permitted web mail service which may be used for company business is the PeoplePlus Outlook Web Access service. Under no circumstances should any other web mail service be used (e.g. Hotmail, Yahoo mail etc) to conduct company business or send any company related information. These services do not provide adequate security controls and also do not project the professional image required by PeoplePlus. In addition the storing of personal data in such mail accounts may constitute a breach of the Data Protection Act 1998.

Confidential Information

In general, and where you are authorized to do so, you may use the PeoplePlus email system to communicate confidential business information internally. However, communicating confidential information outside of PeoplePlus requires special consideration. Please see the Information Labelling and Handling Policy on the Intranet for more information regarding the appropriate handling of confidential information.

If you are still in doubt as to whether to send certain information via email, check with your immediate manager first, or alternatively with the Head of Assurance.

Email Accounts

All email accounts maintained on our systems are the property of PeoplePlus. Passwords MUST NOT be shared with any other individuals. You are responsible for the protection of your logon credentials, which includes your password. Email accounts which remain inactive for long periods of time may be disabled. Accounts may then subsequently be deleted and there should be no expectation of recovery of any lost personal information held within email accounts.

System Monitoring

The contents of our IT resources and communications systems are our property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, stored or recorded on our electronic information and communications systems.

Misuse of the email facility can have a negative impact upon employee productivity and therefore the reputation of PeoplePlus. All of PeoplePlus's email resources are provided for business purposes. Therefore, PeoplePlus maintain the right to examine any systems and inspect any data recorded in those systems.

We reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities. By stating that you have read and understood this policy, you are consenting to such monitoring of your use of such resources and systems.

This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems as well as keystroke capturing and other network monitoring technologies.

We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

Monitoring will comply with the Human Rights Act 1998 and the provisions of the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
Monitoring will only be carried out where necessary, justified and proportionate to the circumstances to:

- Establish facts relevant to the business;
- Check employees' compliance with the law and PeoplePlus policies and procedures;
- Prevent or detect crime;
- Investigate or detect unauthorised use of the telecommunications system;
- Ensure the system's effective operation.
- Determine whether or not communications are business-related;
- Monitor the volume of communications to helplines such as IT Helpdesk and Customer Services.

Information gathered by PeoplePlus in this way may be used in disciplinary, civil and/or criminal investigations.

- PeoplePlus will not (unless required by law or under term of contract):
- Allow third parties to monitor the IT systems
- Disclose information obtained by such monitoring of the IT systems to third parties.

PeoplePlus may be prohibited by law from notifying employees using the IT systems of a disclosure to third parties.

In order to ensure compliance with this policy, PeoplePlus uses monitoring systems to check upon the use and content of emails. Such monitoring is for legitimate business purposes only.

Where it is believed that an employee has failed to comply with this policy then this could lead to disciplinary action being taken.

Disclaimer
The following disclaimer must be used on outgoing email:

"PeoplePlus Group Limited, A Staffline Company (registered number 05722765) Registered Office: 19-20 The Triangle, NG2 Business Park, Nottingham, NG2 1AE.

The information transmitted in this email is intended only for the person(s) or entity to which it is addressed and may contain proprietary, confidential and/or privileged material. Any offers and/or commitments made within this document are subject to contract and without prejudice. If you have received this email in error, please contact the sender by replying and delete this email so that it is not recoverable. Any opinions expressed in this email are those of the individual are not necessarily Staffline Group PLC.

Staffline Group PLC – Registered in England Number: 5268636. Registered Office, c/o Staffline Group PLC, Unit 19&20, The Triangle, Nottingham, NG2 1AE.

Although this email and any attachments are believed to be free of any virus, or any other defect which might affect any computer or IT system into which they are received and opened, it is the responsibility of the recipient to ensure that they are virus free and no responsibility is accepted by the sender for any loss or damage arising in any way from receipt or use thereof.

Staffline Group plc reserves the right to monitor and control email messages sent to and from this address for the purpose of detecting any unauthorised use of its systems and ensuring its effective operation.

Further information about Staffline Group plc can be obtained from www.staffline.co.uk

Legal Risks

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

- If you send/forward emails with any libellous, defamatory, offensive, racist or obscene remarks, you and PeoplePlus can be held liable.
- If you unlawfully forward confidential information, you and PeoplePlus can be held liable.
- If you unlawfully forward or copy messages without permission, you and PeoplePlus can be held liable for copyright infringement.
- If you send an attachment that contains a virus, you and PeoplePlus can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in this Email Policy, the user will be fully liable and PeoplePlus will disassociate itself from the user as far as legally possible.

3.4 Internet Usage Policy

PeoplePlus provides access to and encourages the use of the vast information resources of the Internet as it will assist you to do your job and to be better informed. The Internet can give you a quick and easy route to information about local businesses, national businesses, demographic and other community information.

The facilities required to provide Internet access represent a considerable commitment of resources by PeoplePlus and are primarily provided for business use.

This policy is designed to help you to understand the group's expectations for the use of those resources and to help you use these resources wisely. The terms of this policy shall be understood by and shall apply to all individuals in the PeoplePlus,

including all PeoplePlus employees, contractors, consultants, people working for the group on a self-employed basis, work experience students or other visitors. Failure to observe any of the provisions of this policy could lead to disciplinary action up to and including summary dismissal.

Please note that unlawful Internet usage may generate negative and damaging publicity for PeoplePlus and could expose it to significant legal liabilities.

PeoplePlus's Internet facilities and computing resources must not be used for any illegal purpose or violation of its regulations, policies or procedures

3.4.1 Personal Use

The Internet is, first and foremost, a business tool and PeoplePlus expects you to use your Internet access for company business related purposes. However, a small amount of personal use is permitted but it should be noted that this should be considered a privilege and not a right.

Any personal use of the internet should be outside of core business hours including after/before work and during lunch times and be should approved by your line manager. Any personal financial transactions carried out using the internet will be at the employees own risk.

ICT facilities shall not be used for the purpose of accessing, storing or distributing material that may be considered offensive. In particular, unacceptable use or behaviour includes, but is not limited to the following:

- Visiting Internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- Using PeoplePlus's IT resources to perpetuate any form of fraud, or software, movie, or music piracy
- Using PeoplePlus IT resources to conduct a private business
- Using the Internet to send offensive or harassing material to other users
- Downloading any copyrighted materials belonging to third parties
- Downloading of software from the Internet without the approval of the ICT department
- Gaining access to unauthorised areas or sites
- Publishing defamatory and/or knowingly false material about PeoplePlus, it's employees and/or its customers or suppliers on social networking sites, blogs, wikis or any other online publishing platform
- Revealing confidential PeoplePlus information in a personal online posting, upload or transmission, including financial information, information relating to our customers, business plans, policies, employees, and/or internal discussions
- Undertaking deliberate activities that waste staff effort or networked resources
- Introducing any form of malicious software into the PeoplePlus network
- Using PeoplePlus IT resources including access to the Internet in such a way that it contravenes any UK legislation.

Access to certain social networking sites may be granted for business purposes in accordance with the Social Media Policy.

Prevent Duty and our Responsibilities

PeoplePlus has a duty to protect its staff, learners and customers from any forms of radicalisation and extremism. As a company, we are committed to doing everything we can to comply with this duty and to safeguard our staff, learners and customers.

Background – The Prevent Duty and relevant legislation

'Prevent' is one strand of the UK Government's CONTEST counter-terrorism strategy. The aim is to stop people becoming terrorists or supporting terrorism. This strategy was introduced in 2011. In 2015, The Counter-Terrorism and Security Act 2015 became law in the United Kingdom; it introduced a series of measures designed to tackle radicalisation. As a supplier of public services we must adhere to the Prevent Duty and the Counter-Terrorism and Security Act.

'Prevent' duty guidance was implemented in the further education and skills sector in 2015. As a result, all further education and skills providers in England must have 'due regard' to the need to 'Prevent' people from being drawn into terrorism. PeoplePlus have a statutory duty to stop people from being radicalised and drawn into terrorism (especially in relation to classroom based learners, Apprentices and Offender learning).

It is our duty and responsibility as a company to ensure our learners, customers and staff are protected from radicalisation and extremism. We respond to this requirement in relation to IT in the following ways:

- Blocking web content on all PeoplePlus devices accessible by the internet which may be considered a risk
- Blocking web content on all external devices that are accessed via our internal wifi systems
- Maintain a log of all internet requests regarding prohibited content
- PeoplePlus may release personal and/or confidential information usually protected by the Data Protection Act in instances where a serious criminal act could be prevented especially where others may be endangered, for example an act of terrorism.

3.4.2 Monitoring

PeoplePlus accepts that use of the Internet is a valuable business tool. However, misuse of this facility can have a negative impact upon employee productivity and the reputation of the business. In addition, all PeoplePlus's Internet related resources are provided for business purposes. Consequently, PeoplePlus retains the right to monitor the volume of Internet and network traffic together with the Internet sites that are being visited although the specific content of any transactions will not be monitored unless there is a suspicion of improper use.

Part of this monitoring process includes filtering software that specifically disallows access to certain categories of website, including gambling, pornographic, hatred, and sites with illegal content etc. Due to the nature of this software you may find you have been blocked from accessing certain websites that you consider to be legitimate for business purposes. If this is the case, please raise a call with the ICT Helpdesk to resolve the problem.

3.4.3 Security

Security shall be everyone's first concern and users should note that they can be held accountable for any breaches in security or confidentiality.

4 Information Asset Management

4.1 IT Asset Management Policy

PeoplePlus has a significant information technology asset base consisting of static and mobile assets which are distributed across a nationwide network of locations. It is imperative to the company to exercise proper management of our technology assets at every stage of the asset lifecycle in order to reduce financial and security risks and comply with our legal obligations. As such, this policy provides the governance framework for the whole lifecycle management of the company's IT assets, from Procurement through to eventual disposal.

4.1.1 Acquisition and Procurement of IT Assets

- Requests for IT hardware and software resources must be submitted via the approved process.
- IT hardware and software assets must only be purchased via the approved Procurement process for IT Assets.
- When suitable stock is available, existing assets may be used to fulfill requests.

4.1.2. Asset tagging and recording

- IT hardware assets must be tagged as per the Asset Tagging and Recording Policy.
- Records of specified IT hardware must be kept in an appropriate database as per Asset Tagging and Recording Policy.

4.1.3 Software Asset Management (SAM)

- Software Assets will be managed as per SAM Policy
- All requests, purchases and installations of software must comply with the SAM Policy.

4.1.4 Operational Management of IT Assets

- Users of PeoplePlus IT Assets must comply with all relevant associated policies detailed within the Information Security Policy.
- All employees have a duty of care to ensure IT assets they use are secure, maintained (kept clean, report faults), and kept in a reasonable condition (wear and tear accepted).

- Local managers are responsible for deciding how locally deployed assets are used including where they are used (which room/desk), who uses them, and for what purpose they are used for.

4.1.5 Asset costs

- Costs associated with IT assets (purchase, lease costs, line rentals, depreciation) are billed to cost centre.
- Cost centre managers are responsible for reconciling assets charged to assets deployed in their area of responsibility.
- IT Support Services will assist with rectifying discrepancies and performing audits.

4.1.6 Inactive assets

- PC devices (desktop and laptop computers) are expected to be configured and used on our corporate network (via VPN for laptops).
- PC devices that do not connect to any of our corporate network systems for a period of 8 weeks will be considered inactive and surplus to their current location or role.
- Local managers are obliged to communicate surplus assets to IT Asset Management
- IT may remotely disable inactive assets to prevent security risks
- IT Asset Management may redeploy inactive assets to where there is greater demand for those devices regardless of which department or location they originate.

4.1.7 In-lifecycle changes

- Changes to IT hardware, software and configurations must be submitted and completed by following the approved change control process.
- This includes but is not limited to movement of static IT assets (desktop computers, monitors, printers etc), change of users for mobile assets (laptops, smartphones, dongles etc), changes to cost centre charged, changes to hardware or software configuration
- Records of IT Assets must be updated in response to approved changes as per change control process.
- Any changes occurring that have not followed the change control process will result in assets being disabled or site connectivity to the corporate network being disabled.

4.1.8 Lost and Stolen Assets

- Lost and stolen assets must be reported and dealt with as per Lost and Stolen Assets Process.

- Local managers are responsible for reporting loss of static IT assets in their area of responsibility.
- Staff individually assigned IT assets are responsible for reporting loss of their assets

4.1.9 Recovery of assets from staff leaving the company

- IT assets must be recovered from users leaving the company as per Mobile IT Assets Recovery Policy and process
- Line managers are responsible for recovering IT assets from their users leaving the company
- IT assets recovered from staff leaving the company must be returned to IT Support Services
- IT assets may be remotely disabled until they are returned to IT Support Services

4.1.10 Asset Disposal

- PeoplePlus must meet its legal and contractual obligations to dispose of assets in a responsible manner and in a way that ensures data security
- Assets must be disposed of using only approved suppliers by arrangement through IT Support Services.
- All employees must follow the IT Asset Disposal Process. Local Managers are responsible for ensuring redundant assets are reported.
- PeoplePlus users must not:
    - Independently dispose of IT assets,
    - Donate IT assets to staff, clients or charity or
    - Sell IT assets to staff, clients or any other third party outside the approved IT Asset Disposal Process
- All data bearing devices and media must be disposed of via a route which includes a certified data wipe to relevant legal and contractual standards, and must include asset reporting to maintain an audit trail and proof of disposal.
- Suppliers dealing with IT asset disposals must be reviewed and/or audited annually by PeoplePlus's Procurement or Assurance units to verify the supplier is compliant with all requirements.
- After a certified data wipe (or HDD destroyed), assets for disposal may be routed: Back to lease agent as appropriate, for remarketing to regain any residual value or for recycling where no lease exists and no residual value from resale

Please note that the process for asset disposals from secure prison environments must be referred to local Ministry of Justice IT and Information Security staff. PeoplePlus will comply with their requirements before any movement of assets for disposal.

4.2 Information Classification & Handling Policy

PeoplePlus holds and processes a variety of information as part of providing services to our customers and clients. The company and all of its staff, subcontractors and third parties have a duty to protect our information assets in order to ensure our compliance with relevant legislation including the Data Protection Act 1998, contractual obligations and to fulfil our duties to our clients and customers.

This policy identifies the levels of classification for information assets owned or managed by the company. Information asset 'owners' shall be responsible for assigning classifications to information assets according to the standard information classification system presented below. Where practicable, the information category shall be embedded in the information itself. All third parties handling information on behalf of the company shall be guided by the information category in their security-related handling of PeoplePlus information. All company information and all information entrusted to the company from third parties falls into one of three classifications in the table below, presented in order of increasing sensitivity. When information is not marked as "Public" or "Sensitive" it is implied that the information is Confidential and all controls described in this policy must be applied to it.

The classification will determine the required security controls and handling conditions for the information concerned. A secure storage solution includes:

- Locked metal cabinets where access to keys is only provided to limited number of authorised personnel.
- Locked desk drawers (or other similar storage furniture) where access to keys is only provided to limited number of authorised personnel. Users should not use this type of storage for long term use.
- Locked room accessed by a key or a coded door lock where access to keys and/or codes is only provided to a limited number of authorised personnel
- Role based, access controlled and encrypted electronic devices and medias.

Where access to physical files containing confidential information is required on a frequent basis and therefore maintaining locked drawers or cabinets at all times is impractical, steps must be taken to ensure that authorised personnel are in attendance at all times when the storage facility is unlocked or in use. Similarly, files containing confidential information must never be left unattended whilst removed from their normal locked storage. Personnel handling information classified as confidential should that they follow the requirements of Section 6.1 Clear Desk and Screen Security Policy.

Visitors to areas that contain or process confidential information should be closely monitored and should be signed in and out. The visitors should always be accompanied or supervised in restricted areas.

4.2.1 Information Classifications

Information Category	Description	Examples
Public	Public Information is not confidential and can be made public without any implications for the company. Loss of availability due to system downtime is an acceptable risk. Integrity is the most important element of this information.	Information widely available in the public domain including publicly available company web site areas. Newsletters for external transmission.
Confidential	Information collected and used by PeoplePlus in the conduct of its business to employ people, to fulfil customer contracts, and to manage all aspects of corporate finance. Information received from/or about customers in any form for processing in production by PeoplePlus. Personal Information about staff. The highest possible levels of integrity, confidentiality, and maximum availability are critical.	Customer media. Electronic transmissions from customers. Personal Data pertaining to individuals as per requirements under the Data Protection Act 1998. Information Security risk assessment documentation. Salaries and other personnel data. Documentation relating to security incidents Accounting data and internal financial reports. Confidential customer business data and confidential contracts.

		Non-disclosure agreements with clients\vendors. Company business plans. Passwords and information on corporate security Procedures. Firewall rule set information. Know-how (including forms, templates, training material and presentations) used to process client information. Standard Operating Procedures used in all parts of Company's business. All company developed software code.
Sensitive	Paper based and electronic client personal information provided by DWP/DELNI/MOJ etc which is deemed as sensitive. Such information is only deemed sensitive if the information is received from DWP/DELNI/MOJ etc as a sensitive case. Due to the nature of this information the confidentiality of the information is critical as a loss of confidentiality can have extremely serious implications for the client concerned.	Customer files containing paperwork deemed as Sensitive Cases by DWP/DELNI/MOJ etc. Customer records on systems deemed as Sensitive Cases by DWP/DELNI/MOJ

4.2.2 Information Handling Rules

Classification Label	Handling rule	Disposal Rule
Public	All documents must be marked as public. All removable media containing only public information must be marked as public. The company Communications team must authorise assigning of 'Public' Classification and any subsequent information release	None
Confidential	Store in fixed lockable containers when not being used or when unattended. Distribute only to those who 'Need to Know'. Only release to named and authorised 3rd Parties where 'Non-Disclosure Agreements' are in place. Information only to be processed by personnel, systems or sites approved for this purpose. Minimal copying allowed and must be approved by appropriate manager. Information to be stored in as few places or documents as possible, and for as short a time as possible.	Paper: Shred all copies using a cross cut shredder (minimum standard DIN4) or utilise a secure offsite shredding service. Magnetic Storage (Operational): Subject to destruction using a SEAP 8200 accredited organisation Optical Storage: Shred/crush media using a SEAP 8200 accredited organisation Electronic (Flash) Storage: Overwrite media several

	Personal data relating to clients or staff must be encrypted. Such data **must not** be sent outside the organisation via email or any other means unless authorised in writing by the Regional Director. In these circumstances it must be encrypted. Due to the various requirements of our third parties the encryption tools used will vary. In light of this the Head of Assurance must be consulted to ensure the encryption solution being deployed is appropriate. Where users are required to print or take t hard copies of outside of a PeoplePlus office appropriate security measures must be taken to guard against theft, inappropriate access or accidental loss, damage or destruction of the data	times using an approved tool
Sensitive	Store in fixed lockable containers in non-public areas when not being used or when unattended. Distribute only to those who 'Need to Know' with the authority of the centre manager. Never released to 3rd Parties under any circumstances other than when required in cases of law enforcement. No copying of files permitted. Must never be stored electronically. All files and paperwork must be marked as "sensitive"	Paper: Shred all copies using a cross cut shredder (minimum standard DIN4or utilise a secure offsite shredding service. Permission must be obtained from the centre manager before destruction of such records.

	Files must never be taken offsite except where they are to be transported to another PeoplePlus site. In this case a secure procedure must be followed and the move authorised by the Head of Assurance. A check in procedure must be in place to ensure all files are returned to their secure storage area at the end of each day.	

5 Access Control

5.1 Access Control Policy

PeoplePlus controls access to information on the basis of statutory, contractual, business and security requirements. Access control rules and rights to applications, expressed in standard user profiles, for each user or group of users will be clearly stated, together with the business requirements met by the controls, in the Access Control Matrix.

The security requirements of each business application are determined by a risk assessment that identifies all information related to the application and the risks to that information.

The access rights to each application will take into account:

- The classification levels of information processed within that application and ensure that there is consistency between the classification levels and access control requirements across the systems and network;
- Data protection and privacy legislation and supplier contractual commitments regarding access to data or services;
- The “need to know” principle (i.e. access is granted at the minimum level necessary for the role);
- “Everything is generally forbidden unless expressly permitted”;
- Rules that must always be enforced and those that are only guidelines;
- Prohibit, by restricting access to admin functionality, user initiated changes to information labels;
- Prohibit unauthorised changes to user permissions;
- Enforcing, using up policies and application functionality, rules that require specific permission before enactment;
- Any privileges that users actually need to perform their roles, subject to it being on a need-to-use and event-by-event basis.

PeoplePlus has standard user access profiles for specific system and organisational roles in the business which share common resource requirements.

Management of access rights across the network is managed by the IT Support Desk/Application Support Desk (in the case of system access) and the System Owner (in the case of Application access) following the User Registration Procedure. User access requests, authorisation and administration will be segregated as detailed in the User Registration Procedure. User access requests will be subject to formal authorisation, to periodic review and to removal as detailed in the User Registration Procedure. PeoplePlus will deactivate User IDs and terminate access rights as soon as possible when a staff member leaves the business.

5.2 User ID & Password Policy

The purpose of this policy is to supplement the requirements of Section 4.1 Access Control Policy, through the use of User ID's and secure passwords, to help ensure that access to PeoplePlus ICT and Information Systems is controlled and that only those who have a need to access specific information/systems may do so.

All user login details are unique and assigned to individuals. Under no circumstances should logins be shared.

PeoplePlus recognises that passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire network. Consequently, all users (including contractors and vendors with access to the Network) are to comply with this password policy when selecting and securing passwords.

- Passwords are to be at least 9 characters in length;
- Passwords are to include upper and lower case letters, numbers and special/punctuation characters (using at least 3 of the 4 character types listed);
- Passwords must be changed every 65 days, or immediately where compromise is suspected;
- Passwords issued to new users and other temporary/reset passwords provided by ICT staff must be changed immediately after first use/logon;
- Passwords must not be re-used/recycled;
- Group passwords are not to be used;
- User accounts will be locked out after 5 failed logon attempts and locked accounts should be restricted to administrator password reset;
- ICT staff members are to ensure that pre-set Vendor/Default passwords are changed prior to systems/assets being taken into use;

- All network/system level passwords (including switches, firewalls, servers etc.) are to be changed on termination/departure or change of employment of ICT staff.

Passwords must **not** be:

- shared with others including ICT staff, line managers or others claiming they need to know it for Company/technical/official purposes. If pressed refer demander to this policy.

- written down or stored on-line.

- based on personal information, names of family, etc.

- a dictionary word (any language), slang, dialect, jargon etc.

This password policy is to be applied to all systems within the PeoplePlus network except where individual bespoke applications/systems are incompatible (eg Web Expenses; ProActis).

Although Company policy requires a minimum of only 9 characters, the use of longer passwords is encouraged where systems permit; the longer the password, the more secure it is likely to be. A suggestion is to take all or part of a sentence, saying, phrase etc and abbreviate it.

Users are strongly encouraged to make use of such passwords as they can be easy to remember and virtually impossible to guess.

Passwords are considered to be *weak* if:

- The password is a word found in a dictionary (any language). Hackers often use the Dictionary Attack technique for guessing passwords through the use of computer programs which attempt to crack passwords or passphrases by trying every entry in a given dictionary.

- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms, names, commands, sites, hardware, software.
  - Personal information such as birthdays, addresses, phone numbers.
  - Word or number patterns (aaabbb, qwerty, 123321 etc).
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (eg secret1, 1secret).

Initial temporary one-time passwords are issued by Application Support Help Desk in accordance with the PeoplePlus ICT Account Password Issue Procedure. All Users are to be familiar with this procedure.

Improper use of passwords is to be reported immediately to the Head of Assurance.

5.3 Remote Access Security Policy

Remote access to PeoplePlus information systems, network and resources will only be permitted providing that authorised users are authenticated, data is encrypted across the network, and privileges are restricted.

All remote connections to the company network will be subject to logging to cover account logon time, account logoff time, password resets and login failures.

The company remote access authentication credentials will not be shared or given to any other person, including line managers. Essential to the security of a system is the ability to identify the user, either human or computerised, and if necessary, validate that identity to ensure they are authentic and are in fact who they say they are. Once this authentication has been carried out, controls within the system will ensure they are only able to access systems, data or services for which they have been authorised.

The company service employees and contractors with remote access privileges are only allowed to connect using business-owned computing devices in line with company policies.

All computing devices connecting to the company network remotely will have up-to-date anti-malware software and malware signatures installed by ICT. Such anti-malware software will be fully enabled.

Company owned devices connecting remotely in order to carry administrative tasks on the company network will have an operational personal firewall installed by ICT on their computing devices.

All devices connecting wirelessly to the company network will have a personal firewall installed by ICT which will be fully operational.

6 Cryptography

6.1 Encryption Security Policy

Loss, theft or unauthorised disclosure of could be detrimental to PeoplePlus and its stakeholders. PeoplePlus supports the use of encryption to protect confidential and sensitive information. Data and information, other than that classified as Public, as determined in Section 4.2 Information Classification and Handling will always be transmitted in encrypted form other than in those cases where unencrypted email exchange has been specifically mandated by the relevant Data Controller/Funding Body. Prior to transmission, consideration will always be given to the procedures to be used between the sending and recipient parties and any possible legal issues from using encryption techniques. If staff members are in any doubt as to whether encryption is required or require assistance to encrypt a message or document assistance is available from IT Helpdesk. Staff members should be aware that password protection of a messages or document does not provide sufficient security and is not an approved form of protection.

The lending to external parties of cryptographic private keys, that belong to the company is prohibited.

The management of cryptographic keys and certificates, used to control the encryption, decryption and signing of sensitive information will be performed under dual control, with duties being rotated between authorised company staff. All paper or removable media based keys must be stored in a safe and access to the safe must be limited to only those who are authorised to have access to the cryptographic key.

The impact of encryption and decryption implementation in the company infrastructure will always be assessed with regards to overall performance and availability needs of the business.

Proven, standard government approved algorithms, such as Triple DES and AES will be selected as the encryption algorithms. AES with a minimum key length of 256bit is the preferred encryption algorithm, where possible and practical. SSH is the preferred encryption protocol for peer-to-peer encryption.

Encryption passwords for all databases must have a complex password generated by a random strong password generator such as that found at http://strongpasswordgenerator.com. The password must have a minimum length of 21 characters and include symbols.

Proprietary encryption algorithms are not allowed for any purpose.

Strong keys will always be used when implementing encryption mechanisms, e.g. Transport Layer Security (TLS).

Desktops and laptops, within the company, that contain confidential and sensitive information will have a proven hard disk encryption product installed to prevent compromise of confidentiality, in case of theft.

Clear cryptographic key management solutions will be implemented with the Head of Assurance holding the role of Crypto Custodian. The Crypto Custodian is responsible for ensuring all cryptographic solutions are suitable to the risks identified and to ensure that keys are held in a secure manner under dual control.

Encrypted devices or encryption software must not be taken outside the UK without prior discussion and agreement with the Head of Assurance. This is because certain countries have specific legislation which does not permit the import of certain encryption types. Please note that smartphones are encrypted devices.

7 Physical and Environmental Security

7.1 Physical Security Policy

To ensure that PeoplePlus is compliant with applicable standards, regulation legislation and best practice in the application of "Physical Security" to its employees, its locations and the assets contained within them the provisions of this policy must be followed. Non-compliance may incur reputation, financial and/or physical loss to the business and the possibility of harm to an individual or group of individuals.

Physical security forms the basis for all other security efforts, including personnel and information security. A solid physical security foundation protects and preserves information, physical assets such as PC's, laptops and office equipment as well as human assets, the employees, customers and contractors.

PeoplePlus seeks to safeguard its information, physical assets and human assets by putting in place, or building into design, measures that prevent, deter, delay and detect, attempted or actual unauthorised access, acts of damage and/or violence, which trigger an appropriate response. Physical security involves the appropriate layout and design of facilities, combined with suitable security measures, to prevent unauthorised access and protection of the company's assets, people, information, materials and infrastructure. Physical security involves a number of distinct security measures which form part of a 'layered' or 'defence in depth' approach to security, which take into account the balance between risk prevention, protection and response. Physical security measures, or products such as locks and doors, are categorised according to the level of protection offered.

The 'layered' approach to physical security starts with the protection of the asset at source (e.g. creation, access and storage), then proceeds progressively outwards to include the building, estate and perimeter of the establishment. Approach routes, parking areas, adjacent buildings and utilities/services beyond the perimeter should also be considered. To ensure appropriate physical security controls, the business will consider the following factors:

- The impact of loss of the site or asset
- The level of threat and/or risk
- The perceived level of site or personal vulnerability
- The value, protective marking or amount of material held
- The particular circumstances of the establishment, including considerations of environment, location and whether occupancy is sole or shared

7.1.1 Storage of sensitive assets

Critical, sensitive or protectively marked assets, like laptops, memory sticks, customer files or employee personnel records must be located in secure areas, protected by appropriate entry controls. Where there is a need to store large amounts of inherently valuable removable items, a “Secure Room” must be used.

7.1.2 Office areas

A clear desk policy as detailed in Section 6.1 Clear Desk and Screen Security Policy has been adopted for all offices. This is primarily to ensure that sensitive material such as customer files or personal staff information is not left unattended. Where it is not possible to implement a full clear desk policy, a risk assessment should take place and the decision recorded. The same principle should apply to computer screens and other office areas used to display potentially sensitive information, such as walls, notice boards etc. Computer screens should not be sited where they could be illicitly viewed (e.g. overlooked by windows or reflective surfaces, privacy filters should be used where devices are located in areas used by visitors and when the device is used in a public area.

7.1.3 Building security

In any company building or location there should be as few points of exit and entry as the functions of the site and safety will allow. Where these exist, physical security controls, such as window bars, grilles, shutters, security doors etc., should be installed according to the level of risk/threat. The effectiveness of such controls may be enhanced by the use of intruder detection systems or guard services.

When choosing from the many physical security measures available, business units in conjunction with the Facilities Team should ensure that security controls are able to mitigate violent acts and deter, detect or delay intrusion – those who are not deterred should be forced to use tools and methods that facilitate detection and delay.

7.1.4 Physical access control

Access control refers to the practice of controlling and monitoring access to a property or asset. Physical access control can be achieved through a combination of manned guarding, and mechanical or technical means such as mechanical key pads or electronic door release mechanisms.

Frontline staff, play a vital role in controlling access, but to be fully effective, they may need to be supported by robust customer/visitor/contractor control systems.

Frontline staff, are likely to be exposed to a higher level of risk than others. This should be considered in the risk assessment and additional protections should be put in place as required including lone working arrangements and off-site visits to customers.

7.1.5 Incoming and Outgoing mail and deliveries

Incoming mail and deliveries can include letters, packets and parcels. Each location should have arrangements to store mail securely if it cannot be distributed the recipient.

Outgoing mail can include any letters, packets and parcels sent by post, courier of by hand of a member of staff. When using postal or courier services documents must be set in batches rather than on an individual basis but should not be stockpiled. Outgoing mail arrangements should follow the following principles:

- Always used a tracked service when sending personal data of about 20 or more individuals together.
- Reference should be made to funding body guidance e.g. DWP Provider Guidance Chapter 8

7.1.6 Manned guarding

If it is determined by a business unit in conjunction with the Facilities Team that on-site manned guarding is necessary the primary role of the Guard must be to provide deterrence against hostile activity and facilitate a rapid response to security incidents not to supplement Reception Staff. Guard duties and the need for, and frequency of, patrols should be decided by considering the level of threat and any other security systems or equipment that might already be in place.

7.1.7 CCTV

Where it is determined by a business unit in conjunction with the Facilities Team and Data Protection Officer that CCTV is required the location must be particularly aware of the Data Protection Act Principles and the Information Commissioner's Code of Practice on CCTV, which is published under the Act.

7.1.8 Intruder Alarms

If it is determined by a business unit in conjunction with the Facilities Team that than intruder alarm is required an appropriate cost benefit analysis should be performed.

7.1.9 Photography, Audio and/or Video Recording

The taking of photographs or making audio and/or video recordings on PeoplePlus premises is strictly prohibited, unless it is covered by the following exceptions:

- Photography, Audio and/or Video Recording for use in marketing material. If photography or filming is scheduled to take place in any PeoplePlus Office signs should be placed around the office to make employees, customers and visitors aware that recording is in progress give the option to be excluded from shots. Customers should be required to complete a media consent form.

- Photography, Audio and/or Video Recording for continued evaluation of employee skills, knowledge and proficiency especially for employees working within the Money Advice Service.
- Photography, Audio and/or Video Recording for purposes of assessment of learners/customers/employees performing training or a completing a qualification.
- Photography, Audio and/or Video Recording where express permission has been granted by the Head of Assurance.

Where permission is granted to a customer or third party, the request should be submitted in writing and, clearly state purpose(s) for which the recording / photography will be used. Please note that where permission is granted, it is still subject to the requestor obtaining permission from the individual(s) who will appear in the photographs or recordings, if this has not been obtained, the requestor will be unable to obtain photographs and/or recordings.

You should always obtain the permission of the person(s) who will be in the photograph/video/ audio recording and document their consent and place this on their record before you photograph or record them. If the individual is below the age of 14, then their guardian should also provide their formal consent and both consents should be retained on file.

It is strongly recommended that where this type of media is used that you develop and implement processes that clearly define the purpose for gathering data this way, as well as the retention period, when and how they will be stored and/or destroyed. Please note that evidence of destruction may be required.

If determined necessary by the Information Security any requirements around physical security will be included in an annual Penetration Test in accordance with the Penetration Policy.

7.2 Equipment Security Policy

All PeoplePlus equipment will be securely managed in order to control any security risks that may incur loss to the business. Equipment is defined as hardware devices owned by the company to include PC's and laptops, printers, fax machines, scanners, hard disks, servers etc. Mobile computing devices such as laptops, mobile printers, personal digital assistants and smart phones are addressed in Section 14.2 Mobile Phone Usage Policy.

The procurement of all equipment must be approved by the IT Department before being purchased through appropriate channels. Equipment not purchases in this way must not be installed as it could constitute a security breach. Any movement of such hardware defined above from its recorded company location will be strictly controlled by authorised ICT department personnel.

The company equipment will be formally "signed for" when removed from the premises to be in control of its location, expected return and overall security.

Equipment used by Field Operations Staff will be appropriately controlled and approved by line managers.

Once proper authorisation has been obtained, the physical security of the equipment and the security of any information contained on it will be assessed and addressed, before taking company equipment off site.

Only authorised personnel are permitted to take equipment belonging to the company off premises - they are responsible for its security at all times.

This policy will be supported by a procedure regarding the removal of equipment from the company premises.

Field-based Operations Staff and mobile computer users will implement additional supporting procedures regarding secure use and storage of equipment when working on and away from site to limit the risk of theft or loss:

- Keep the mobile computer out of sight when it is not being used. It should be locked away and never left in cars overnight. When travelling by car laptops should be placed in the boot for security
- Keep the mobile computer close at hand and, if possible remain in physical contact with the laptop at all times. If travelling by public transport do not use communal storage areas to store your laptop.
- Take responsibility for your mobile computer by never leaving it unattended in an office environment. Management and users should consider the acquisition and deployment of a device such as or similar to a laptop lock for use whilst mobile devices are unattended for short periods of time.

All equipment owned, leased or licensed by the company will be supported by appropriate maintenance facilities from qualified engineers.

The company sites chosen to locate computers and to store data will be suitably protected from physical intrusion, theft, fire, flood and other hazards.

The company equipment will be sited and used to comply with Health & Safety regulations and not block fire exit routes.

The company premises-based computer equipment will be safeguarded against unlawful and unauthorised physical intrusion and theft.

7.3 Disposal and Decommissioning Security Policy

The purpose of the Disposal and Decommissioning Security Policy is to ensure that all PeoplePlus confidential information, ICT systems, and removable media is decommissioned and disposed of in a secure manner the provisions of this policy must be applied. Should information or systems not be subject to suitable disposal confidential information could easily be obtained by unauthorised parties.

Document Destruction

All personal and corporate information processed manually using hard copy paper based records and files that are no longer required should be destroyed in line with contractual and legal obligations. The destruction method should ensure of all records are disposed of in a way which prevents republishing or further distributed. In PeoplePlus this is achieved by disposing of the material in a confidential waste bin which should be emptied on a regular basis by a designated contractor. If a location does not have a confidential waste bin the material must be shredded. The minimum destruction requirement require the shredding of paper based records using a cross cut shredder that cuts the paper into pieces of no more than 15mm x 4 mm.

If a location is closing or a shredder is not available paper based documents containing confidential information should be stored in a secure location usually the confidential waste bin or other secure location prior to being sent for destruction. PeoplePlus only uses approved contractors to collect and dispose of this confidential waste.

Electronic Data Destruction

All personal data must be stored in secure databases and/or systems or secured networks. All IT equipment must be disposed of via the IT department to ensure all confidential is removed and that hard disks are cleared of all software and all confidential information prior to disposal or re-use. The ICT Service Delivery Manager is responsible for the secure disposal of storage media and the disposal of all information processing equipment. All storage media will be disposed of in line with SEAP 8200 guidelines. A log will be retained showing what media were destroyed, disposed of, and when. The asset inventory is adjusted once the asset has been disposed of.

Operational and Support Managers are responsible for notifying ICT of all equipment which requires de-commissioning and disposal. Staff outside of ICT Department are not authorised to destroy or dispose of IT equipment. This includes removable media such as CDs/DVDs, portable hard disks, USB data sticks, SD cards etc.

All equipment awaiting destruction will be stored in a secure area with limited access. A log will be kept of all equipment held in the secure area and such equipment will be subject to random audits.

Devices containing confidential information that are damaged will be subject to a risk assessment from the Head of Assurance to establish whether the device should be repaired or replaced.

Paper based documents containing confidential information will be stored in a secure location prior to being sent for destruction. The company will use approved contractors to collect and dispose of this confidential waste.

Hard disks from photocopying and printing devices will also be subject to secure disposal as per this policy.

Where machines are to be re-deployed internally they will be subject to a re-image using the company's standard build.

Machines issued to external parties such as subcontractors will either be issued as new devices or will have been subject to secure disk wiping using a CESG approved product before being deployed. Such machines remain the property of the company and subcontractors are not authorised to destroy or dispose of these machines.

Network devices such as firewalls, routers and switches will be de-commissioned by the ICT department and will be subject to a secure wiping procedure before disposal.

All equipment will be disposed of in line with Waste Electrical and Electronic Equipment (WEEE) directive. Copies of certificates for the destruction of such equipment will be retained by the ICT Service Delivery Manager.

7.4 Clear Desk and Screen Security Policy

To ensure that information security risks related to unauthorised disclosure of paper and electronic documentation is minimised PeoplePlus must ensure that access to information is appropriately controlled. This section identifies the requirements for controlling access to information.

All offices and PeoplePlus buildings will have facilities to store confidential paper information and physical media in a controlled manner. The facilities will include cabinets, with lockable desk drawers for temporary shortage, whilst the premises are occupied.

Access to lockable drawers and cabinets will be controlled by the Centre Manager to ensure staff members have access to the physical information relevant to their role. If staff do not have access to lockable drawers/cabinets they should ensure that this is escalated to their Centre Manager.

Critical paper information such as Business Continuity and Disaster Recovery plans will be held in fire-proof safes at agreed strategic locations (identified in the Business Continuity Plans) within the business. The fire-proof safe shall provide a minimum of two hours protection. The access codes to these safes will be limited to those individuals named in the Business Continuity plan.

When staff members leave their desks even for a short period of time the screen must be locked using the Ctrl-Alt-Delete function followed by pressing “lock this computer” or pressing enter or Windows Key-L function and all confidential paper documentation should be locked in the facilities provided.

The Head of Assurance will schedule and coordinate site audits to confirm compliance with the policy.

All ICT equipment will be configured to ensure the screen is locked after a period of ten minutes inactivity.

All machines including, PCs, laptops, printers and photocopiers will be shut down and switched off overnight or when not in use for a prolonged period of time.

Each site will have procedures for controlling incoming and outgoing mail with specific individuals responsible for this area. These procedures will be communicated to all staff at the site to ensure mail and other important documents are at reduced risk of loss or theft. These procedures will also extend to Fax machines. The Office/Centre Manager is responsible for the development of these procedures and for ensuring staff members are aware of the local procedures.

8 Operations Security

8.1 Change Control Policy

All change requests will be subject to review by the ICT department and the Head of Assurance to ensure the proposal remains in line with company policy. The Head of Assurance will consider the impacts upon Information Security and Business Continuity when undertaking the review.

Subject to a satisfactory review request will be formally authorised. Changes which are not authorised will not be made.

All changes will be subject to rigorous testing prior to deployment and will include suitable back out plans.

For further details refer to IT Change Management Policy and IT Change Management Procedure.

8.2 Security Monitoring Policy

The security monitoring of PeoplePlus systems is implemented to deter and detect unauthorised use and abuse of systems. Poor monitoring management is a weakness that may be exploited by internal or external attackers. Such weaknesses may incur loss to the business since intrusions and misuse may go undetected. Operating systems within the company infrastructure will be regularly monitored and all required 'housekeeping' procedures will be performed.

Software faults within the company infrastructure will be formally recorded and reported to those responsible for software support / maintenance.

The use of company information systems will be monitored regularly. Company information will also be periodically audited to identify any security weaknesses.

Each layer within the company IT systems (Physical, Operating System, Middleware, and Application) will host appropriate monitoring to ensure suitable warnings are generated if their Security Access Structures fail.

Access to company information systems will be logged and monitored to identify potential misuse of systems or information (refer to the PeoplePlus Security Audit Policy for more details). System access will be monitored regularly to thwart attempts at unauthorised access and to confirm that access control standards are effective.

The following critical company infrastructure components are amongst those that will be monitored for security incidents:

- Firewalls (External and Internal)
- Web Servers
- CITRIX Access Gateway

- Business Critical back-end servers
- Routers and Switches

The log output from company critical infrastructure components will be collated and analysed to detect any abnormal or suspicious activity, which will be reported to the Head of Assurance who will take necessary action and initiate an investigation, if required.

The Head of Assurance will define the business security monitoring requirements and make appropriate recommendations to Business Management. Following formal business approval, details of business security monitoring requirements will be cascaded to the ICT staff so that they may be incorporated into their work activities. These requirements will form the basis for the monthly security checklist that Security Manager will produce and feed back to the Information Security Forum.

This monitoring will be used in the longer term as part of the overall ISMS information security metrics.

8.3 Anti-Malware Security Policy

The threat posed by the infiltration of virus and malware is high, as is the risk to the company Information systems and data files. Formal procedures for responding to a malware incident have be developed, tested and implemented.

Anti-Virus protection will be available of all PeoplePlus computing devices which will be subject to automatic updates. A centrally managed proven enterprise scale anti-malware solution with scalable deployment functionality meeting the needs of the business will be installed on all computing devices (laptops, desktops, servers and other computing devices) that connect to the company network.

Anti-malware software will be included in the secure builds for all computing devices that connect to the company network.

All new software code to be used by the company will be scanned for viruses before being moved into production or being transmitted/stored on the company network.

Malware signature updates will be obtained from a trusted source at least once daily, from when a new vulnerability and signature is announced by the vendor, tested to ensure that a new signature does not negatively impact the company system infrastructure and then updated on the central anti-malware server.

Malware signature updates will be automatically pushed out to computing devices from a centrally managed point in the company infrastructure.

Anti-malware software will be enabled and configured so that it cannot be tampered with on computing devices that connect to the company network.

Daily reviews shall be undertaken by the ICT department to identify machines which do not have the latest Anti-Malware signatures installed. Where such machines are identified this will be logged with suitable action being taken to identify and resolve the problem as soon as practicable.

The Head of Assurance will present Anti-Malware coverage statistics to each Information Security Forum meeting as one of the key Information Security Metrics.

A malware incident response procedure will be in place to facilitate the removal of any infection with minimal disruption. Such procedures will be regularly reviewed and tested by the ICT team.

System users will take great care when downloading information and files from the internet to safeguard against both malicious code and also inappropriate material.

Employees are not permitted to load non-approved software that is not required by the business onto the organisation's PCs, laptops and workstations. The installation of any software will be authorised and undertaken by the ICT department.

The use of removable media disks and digital devices with memory capability, e.g. disks, flash memory devices, portable hard disks, mp3 players, digital cameras and CD-ROM, is not permitted within the company except where specifically authorised. This also applies to CD recording devices and similar technology.

Mobile code such as Active X and Java Applets will be strictly controlled with such code only being authorised as per business need.

8.4 Logging and Monitoring Security Policy

The Head of Assurance and Information Security Forum will define the business security audit requirements and make appropriate recommendations to Senior Management, who will in turn, approve them as a business requirement.

The company business-critical audit logs will be sized appropriately and their contents reviewed regularly by trained staff, with discrepancies being reported to the business and the owner of the information system.

Nobody, in particular trusted users with high levels of privilege, such as company system administrators, will deliberately make audit logs inoperative or 'de-selected', in order to conceal present or future unauthorised systems activities.

All The company system clocks will be synchronised daily from a single time source, in particular between the various processing platforms within the company infrastructure. The time source server should not be used for any other function and the Network Time Protocol (NTP) deployment will be secured in line with the latest best practice.

Manipulating 'system time' in the company environment is not permitted, since it may invalidate log contents, which might compromise investigation of security incidents under Section 11.1.

The company audit logs and customer data will be safeguarded using a combination of technical access controls and robust procedures, with all changes supported by logging and internal audit controls.

The activities of company system administrators and the use of powerful system utility tools will be audited by independent internal auditors on a regular basis.

The company will implement auditing of all business-critical transactions that create, update or delete data on information systems agreed by the Information Security Forum. This information will be recorded in audit tables which will be available for analysis. Where available this will include:

- User name
- Date
- Transaction Start Time
- Transaction End Time
- Satisfactory completion of transactions which have a financial implication
- Access to and alteration of critical or security data
- Instances when processes are halted because of security or privilege breaches

The company ISO/IEC 27001 Information Security Management System (ISMS) will be assessed by the internal audit team on a bi annual basis.

8.5 PCs, Tablets and Laptop Security Policy

To ensure that all business-critical PCs in the PeoplePlus infrastructure are securely configured and managed to minimise any security risks to the business. Poor configuration and poor management of PCs are weaknesses that may be exploited by internal or external attackers and incur loss to the business. All The company information system users of PCs, Tablets and laptops will lock access to their PC or log off when it is not being used.

The use of personal removable media on company PCs such as mp3 players, memory sticks, portable hard disks and digital cameras is not permitted. The company provide authorised devices where required via the ICT department. All requests to use such devices should be directed via line managers to the ICT department who will provide the appropriate equipment based on business need.

All users of company information systems, whose job function requires them to create or amend data files, will save their work on their network drives regularly in accordance with best practice, to prevent corruption or loss through system or power

malfunction. Data and documents should be stored on the relevant network drive, if you do not have access to a, relevant, network drive, seek assistance from the IT Helpdesk and/or your managers. Local drives a should only be used for temporary storage.

PeoplePlus users are not permitted to load non-approved software onto the company's PCs or laptops. All software requirements will be reviewed by ICT who will procure and install necessary software based on business need. The installation of software without prior permission could be in breach of the Copyright Designs and Patents Act 1988 and may prevent PC's and Laptops from working. Similarly, under no circumstances should laptop users install third party software provided by your personal internet service provider. If you require any support to connect to your laptop to PeoplePlus network through your home broadband contact the IT ServiceDesk

The company PCs and Laptops will be sized according to defined business requirements to meet availability business needs.

The PC configuration will be under strict change control and contained in a standardised secure build. The secure PC build will incorporate security best practice and will be reviewed by the Head of Assurance.

PCs will not have any server services or protocols running or ports listening unless this is required by the business.

Any unnecessary operating system components not required by the business will be removed.

Any unnecessary applications not required by the business will be removed.

External interfaces and devices will be disabled (floppy drive, SD drive, serial port, CD/DVD drive, USB port, Firewire port, infrared, wireless networking, Bluetooth etc) unless there is a business requirement for the interfaces to be enabled. Requests for access to these should be submitted to the IT Service Des, for processing via the Waiver Process.

PC administrative interfaces will be locked down, have access restricted to the management internal network only, apply secure protocols, apply strong authentication and not be exposed to the public network.

When PCs are sited consideration should be given to the physical security aspects of the buildings in which the PCs are used. Any concerns regarding the physical security of equipment should be reported to the Head of Assurance as soon as possible.

All PCs will have Anti-Malware installed and a formal process for automatically updating Malware signatures will be applied (see PeoplePlus Anti-Malware Policy for more information).

There will be a defined formal process for notification of new PC patches, secure download and patch testing and implementation.

PC logs will be protected against unauthorised access and tampering.

All PCs will have warning banners enabled advising users that they are logging onto company owned equipment and that they will adhere to the relevant legislation and company policies.

8.6 Authentication Security Policy

The company will implement authentication mechanisms of the appropriate strength and manage information security risks to the business. The mechanisms will be suited for the delivery channel in question. Information classed above public will not be divulged unless the user has been authenticated and authorised to access the requested information.

8.6.1 Web Authentication

The company web applications will implement a secure mechanism to authenticate all users that access applications through the browser interface. Role-based access control will be implemented in the application and authentication will be implemented using a password mechanism (refer to PeoplePlus Password Policy for more information).

8.6.2 Voice Authentication

Any telephone enquiries requesting non-public information will only be responded to once the identity of the caller has been verified. All contractual obligations in authenticating telephone callers will be complied with prior to any information being disclosed.

Users will be aware of “social engineering” attacks, where the aim is to trick people into revealing passwords or other information that compromises the security of company information. Users will be trained and be able to prevent and report such attack attempts to the Head of Assurance.

This requirement is of particular importance as it forms part of the Data Protection Act 1998.

8.6.3 Email Authentication

Incoming e-mail to the company network will be treated with the utmost care due to its inherent Information Security risks. The opening of e-mail with file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code. Users will be trained and be able to prevent and report phishing and malware attacks

9 Communications Security

9.1 Network Security Policy

The physical location of all network infrastructure devices will be resistant to unauthorised access and tampering, Network infrastructure devices where possible should be stored in secure network cabinets with secure equipment rooms. Only representatives from the PeoplePlus IT department should be permitted access to the network cabinet

Manufacturer defaults such as default SNMP strings and passwords will be changed before network devices are deployed.

The configuration and design of network solutions will be kept as simple as possible. All network devices will have minimal packages and applications installed. The exact number and types of services will be defined during the design stage. Anything that is not required by the business will be removed or disabled. Standardised network device builds/configurations will be applied.

All network devices will have minimal protocols, services running and ports open. Any unnecessary protocols not required by the business will be disabled by the Network Administrator with the authorisation of the ICT Infrastructure Manager.

The use of generic “administrator” accounts on all network devices is prohibited.

There will be a defined formal process for notification of new patches, secure download and patch testing and implementation.

Network devices will be subject to vulnerability assessments at set intervals to identify any configuration vulnerabilities or missing patches.

The company network device logs will be protected against unauthorised access and tampering using suitable access controls and file integrity monitoring.

Logs that are sent to a logging server will be transferred over a secure network and will not be sent in clear text in order to prevent attackers from sniffing logs, and disclosing confidential information regarding the system.

Network device size, and performance will be chosen according to defined business requirements to meet availability, integrity and confidentiality needs of the company service. All installations for network cabling, equipment and telecommunication equipment must be applied for and arranged in advance through the IT department ensuring that they conform to the necessary standards. Requests for changes such as the connection of additional switches or ports should be made through the IT Helpdesk.

A random selection of network device configurations (including firewalls) will be reviewed against the company base build every six months to identify any unauthorised changes.

Network device system clocks will be synchronized with the company service infrastructure (required services for this will be locked down and not accessible from the Internet).

The company network device system clocks will be synchronised with the rest of the company infrastructure, using a single time-source that provides no other function.

Network device administrative interfaces will be locked down, have access restricted to the management internal network, apply secure protocols, apply strong authentication resistant to brute-force attacks, implement strong passwords and not be exposed to the public network.

Network device logging will be enabled in accordance with Section 7.4 Logging and Monitoring Policy. In addition there will be a formal process for the secure back up of firewall logs.

There will be a formal change control applied to the company network device configurations, which will be documented and securely backed up.

Changes to the network device security configuration will be authorised and approved by the Head of Assurance.

Only authorised users are permitted to connect to and make use of the PeoplePlus network. Only devices, which have been issued by PeoplePlus, may be connected to the network as detailed below:

PeoplePlus Laptops and Desktops	Automatically given permission to connect
Data Network Equipment	Prohibited – only to be connected by the IT Department
Wireless Access Points	Prohibited – only to be connected by the IT Department
Servers	Prohibited - unless installed by the IT Department
All other devices	Prohibited – including personal mobile telephony services

9.2 Firewall Security Policy

Failover implementations will meet business requirements defined in the Business Continuity Plan and be tested to ensure effective resilience.

Firewalls will apply ingress (inbound) and egress (outbound) filtering, applied to control traffic to and from the company network.

Firewall configurations will be formally documented, securely backed up and be under strict change control. Requests regarding changes to the firewall configuration will be approved by the Head of Assurance given a genuine business reason exists.

Firewall alerts will be sent to an internal central solution managed by ICT which is responsible for monitoring the firewall and alerting administrators of any activity which could threaten the Confidentiality, Integrity or Availability of the company network.

All firewalls will have a Computer Misuse Act "warning banner" stating that it is unlawful to enter or attempt to enter the company network without proper authorisation.

The firewall implementation and rule-set will be subject to annual penetration testing as organised by the Head of Assurance to ensure that the rules are implemented and effective. Testing should also be undertaken where changes or Information Security incidents have occurred. All Penetration Testing will be commissioned in accordance with the Penetration Testing Policy.

Insecure Internet Control Message Protocol (ICMP) traffic will be restricted to prevent attackers from "firewalking", i.e. mapping the firewall and it's rule-set. ICMP broadcasts will not be routed and will not be responded to. ICMP redirects and ICMP timestamp requests will be ignored.

Source routing will be disabled to prevent attackers from bypassing the firewall.

9.3 Router and Switch Security Policy

Router and switch failover implementations will meet business requirements defined in the Business Continuity Plan and will be tested to ensure effective resilience.

Inbound packet filtering will be applied on router and switch-management interfaces, according to business requirements to restrict unauthorised packets from entering the company network. All illegal, internal, private non-routable addresses will be denied entry to the company network.

Outbound unreachable responses will be blocked to prevent "firewalking", i.e. mapping the network by external attackers.

Loose source routing will be disabled on all company routers and switches by the Network Administrator as authorised by the IT Service Delivery Manager.

Direct broadcast will be disabled on company routers and switches to prevent "smurf" attacks.

The company routers and switches will have a "warning banner" stating that it is unlawful to enter or attempt to enter the network without proper authorization. However, such a banner should not identify the company Organisation.

The company router and switch implementation and security filtering rules will be tested regularly to ensure that the rules are implemented and effective.

9.4 Wireless Security Policy

All new company infrastructure wireless installations will be planned formally and notified to all interested parties ahead of the proposed installation date. Information Security requirements for new installations will be circulated for comment to all interested parties, well in advance of installation.

The company wireless network will be designed and configured to deliver availability and reliability to meet the needs of the business whilst providing an adequate degree of access control and a range of privilege restrictions based on the 'least privilege' principle and job roles.

The company wireless network will be documented in a diagram, which will be kept up to date by the ICT Service Delivery Manager when any formal changes are made.

Out-of-band administrative console access will be provided where ever possible. When this is not feasible, encryption will be used (SSH).

Required Countermeasures to reduce the risk of eavesdropping:

Ensure that 802.11i (strong encryption channel for confidentiality) is used with 802.1x/EAP (Extensible Authentication Protocol). The 802.1X and EAP configuration provides:

- Mutual authentication between client and authentication (Remote Access Dial-In User Service [RADIUS]) server
- Encryption keys dynamically derived after authentication
- Centralised policy control, where session time-out triggers re-authentication and new encryption key generation

Access Points will be sited with care and where possible will not be sited near windows or external walls. Advice will be taken from vendors on suitable positioning. In the conflict between getting adequate coverage within a building and trying to minimise the external radiation the priority is to reduce the external signal.

Where possible only products with selectable power levels will be used with only the minimum power used to provide the required coverage.

Wireless Access Points will not be connected directly to Ethernet hubs. If connected to a hub, the Wireless LAN will transmit all data appearing on the wired LAN, this practice can significantly increase the likelihood of a successful eavesdropping attack.

If used externally, e.g. site to site with directional aerials and wireless routers/bridges, IPSec VPN technology will be used.

Proactive analysis of the network will be undertaken to identify unauthorised or “rogue” wireless access points. Such devices can expose the company network to unauthorised access and pose a significant risk to the company.

Staff and third parties will not connect any wireless device to the network.

Required countermeasures to reduce the risk of illicit connection:

If possible use products with MAC address filtering. Although MAC addresses can be spoofed this represents a further barrier.

All devices which require connections to the wireless network will be authenticated using certificate based authentication.

Management traffic will be limited to a dedicated management wired subnet. Management traffic will be isolated from user traffic and encrypt all management traffic (SSH) where possible. Centralised user authentication (RADIUS) for the management interface will be enabled.

Where possible only strong community strings for Simple Network Management Protocol (SNMP) will be used and such strings will be changed bi-annually or when a member of ICT staff leaves the organisation. Where possible SNMP read only strings will be used if the management infrastructure allows it.

The security of the wireless network will always be included in the scope of the company’s annual penetration testing activities due to the high risk nature of wireless technology.

9.5 External Communications Security Policy

To ensure all information and external communications for PeoplePlus are managed, controlled and properly released at all times. Improper release of information, including incorrect use of Company brands, could harm the reputation of the Company and its corporate image and competitive position in the marketplace.

9.5.1 Public and semi-public places

Employees must not discuss work or any work related matters where there is a possibility of being overheard. The risk of being overhead and divulging protected information exists on trains, in restaurants and in other public places. Likewise, work should not be discussed on PeoplePlus premises and open plan offices where visitors might be present. In such incidences care should be taken to ensure that discussion is not overheard by visitors or customers. Staff must not leave internal documents or other papers relevant to the Company business where they might be found by people who do not work for the Company.

9.5.2 Talking to people outside the company

Staff must not be drawn into talking about work when meeting people from outside the Company in either professional or social situations. Particular care should be taken if approached by a journalist. Under no circumstances should staff give opinions or information about any of the Company's contracts, employees or competitors - there is no such thing as 'off the record'.

9.5.3 Contact from a journalist, MP or other official

The day-to-day responsibility of handling all public and media relations rests with the Marketing and Communications team. If any media or external stakeholders request information about Company services or contracts or would like to visit a Company office, staff must follow a strict procedure to ensure all requests are handled appropriately. This will ensure strong messages are communicated and correct lines of response determined at all times.

- Ask for the name of the caller, their telephone number and the publication or organisation they work for.
- Inform the caller that all external enquires are dealt with by the Marketing and Communications team. Do not attempt to respond or give your own personal opinion
- Give the caller the email address of the Marketing and Communications team pressoffice@peopleplus.co.uk
- Report the request and/or conversation immediately to the Marketing and Communications team at pressoffice@peopleplus.co.uk.

9.5.4 Reporting potential media coverage

Any event or activity that could result in the Company being mentioned in local, regional or national press should be advised to the Marketing and Communications team pressoffice@peopleplus.co.uk. This includes any positive or adverse publicity relating to the Company.

Any incidents must also be reported immediately via the Company Information Security Incident Management process.

9.5.5 Management of all external communications/materials

The Marketing Department is responsible for overseeing and managing the design and production of all external communications and all publicity/media handling on a national, regional and local basis. The Marketing Department will ensure all external materials and activities including advertisements, brochures, leaflets, competition entries, signage, press releases and media interviews, comply with corporate brand

and identity/style guidelines, communicate strong and consistent messages at all times and that the Company remains contractually compliant.

Under no circumstances should staff develop or use any marketing and communication materials without prior consultation with the Marketing Department.

Written confirmation from customers, employers or partner organisations must be obtained before any details (including photos and quotes) can be used in any external communications. Signed authorisation forms must be completed and returned to the Marketing Department.

Under no circumstances, with exceptions for safeguarding disclosures and disclosure that are exempt under the Data Protection Act 1998, must any details relating to customers be disclosed to third parties without their formal consent. Any situations where personal data is to be used/disclosed for any matter other than handled by the Marketing Department should be brought to the attention of the Head of Assurance immediately.

9.5.6 Websites and Online Technologies

The Company websites are managed and maintained by the Marketing Department. Any requests for changes to the content on these websites must be escalated to the Marketing Department.

Staff must not under any circumstances post confidential information websites, online bulletin boards, blogs or social networking sites such as Facebook, Twitter and LinkedIn.

Any staff using bulletin boards, blogs or social networking sites for personal use must not identify themselves as employees of the Company in online profiles and must not express views of the Company without formal authorisation from the Marketing Department.

9.5.7 Partners, Subcontractors and Suppliers

All third parties undertaking external communications or publicity that directly mention or relate to work being carried out on behalf of the Company must work closely with the Marketing Department. Any external communications produced to promote any contract provision or services being delivered on behalf of the Company, such as marketing materials, advertisements and press releases must follow the branding and communications guidelines provided by the Company and must be approved by the Marketing Department.

It the responsibility of the relevant Supply Chain Manager to make sure all partners, subcontractors and suppliers are aware of, and are compliant with this requirement.

10 System Acquisition Development and Maintenance

10.1 Database Security Policy

To ensure that PeoplePlus incorporates best practice into the design and development of Databases the provisions of this policy must be enforced. If risks with regards to common Database vulnerabilities are not properly managed, the business could be exposed to potential information loss or corruption.

10.1.1 Database Development & Design

All system developers will apply security best practice to any Database development processes and design – this applies to both internal and third party Database development.

Database security requirements will be formally defined at the requirements gathering phase for all Database development. The Head of Assurance will be involved in all such projects from an early phase to ensure Information Security requirements are considered at the beginning of the development process.

Databases will not be directly exposed to public or un-trusted networks (i.e. the Internet) nor have database ports open on Internet-facing firewalls.

Changes to Database structure or availability will be controlled by the Database Administrator, following formal change control procedures.

Developers will store their Database code on the server, making it available to authenticated and authorised applications through the use of parameterised queries or prepared statements as opposed to using string queries. This limits the range of actions applications may perform on the database and ensures that risks from injection attacks are minimised.
Developers will never include SQL commands in applications. This creates a significant vulnerability if malicious users are able to later modify the application.
Database design will incorporate locking procedures, designed to avoid multiple simultaneous updates and conditions known as “deadly embraces”. An integrity checking and repairing process will be incorporated into business critical Databases.
Database links will only give access to the required views or tables.
The company Databases will individually identify each user of the system, only permitting access to information/functions necessary for their job role.

Databases will obscure all password entry fields in order to protect passwords from eavesdroppers.

Databases will provide an appropriate level of audit against changes to sensitive information, execution of ad-hoc Database queries and privileged functions.

All Security Auditing database code (including views) will be checked for security risks by the Database Administrator and the Security Manager.

Database applications development and operation will only be performed on properly hardened platforms to ensure that weak operating systems do not undermine the security of the Database.

10.1.2 Database Use & Operation

Applications that access company Databases will only interact with views rather than interact directly with the underlying table. This allows greater control over access to information, both at the row and column level.

Database applications will be subject to appropriate security patching when available. Software updates will be obtained from a trusted source and be tested in a separate environment before being implemented in the production environment.

Database Administrators will have sole responsibility for allocating and modifying Database-user permissions. Developers and other users requiring a change to user permissions will make their request to the Database Administrator, following formal change control procedures where applicable.

Ad-hoc reports against production Databases will only be executed by the Database Administrator.

Scripts will only be executed against live or production Databases following formal acceptance and authorisation, based on a security review and performance impact assessment, from the Database Administrator.

All Security Alerts will be brought to the attention of the Database Administrator, if deemed as suspicious will be escalated to the Security Manager.

Standard default Database usernames will be disabled where possible. All default user passwords will be changed immediately upon Database installation.

Where Database listeners are used, they will have passwords set meeting the complexity requirements of the company Password Policy.

Database agents and processes will always follow the principle of least privilege, having only the privileges needed to perform required tasks, and not run as high privilege accounts and processes.

Live or Production Databases will never be used for the purpose of testing or development. Any changes to the framework or function of a production Database will follow formal change control processes.

Database servers will be scanned with vulnerability assessment tools by an authorised party on a quarterly basis to ensure that up to date patching and secure configurations are applied. The Security Manager will approve this activity before it is allowed to be conducted.

Remote database management will be securely managed restricting access and ensuring that administrative interfaces are properly locked down with secure protocols applied.

11 Supplier Relationships

11.1 Third Party Security Policy

Only properly authorised persons within the company may authorise and approve the use of third party suppliers or subcontractors.

Employees responsible for commissioning outsourced computer processing, software development or service provision will ensure that the services used are from reputable organisations that operate in accordance with clear security standards such as ISO/IEC 27001. PeoplePlus also reserves the right to request compliance other security standards and controls if deemed necessary. Any proposal will be reviewed and approved by the relationship manager with suitable input from the Head of Assurance.

Third party access to company information is only permitted where the proper authentication and authorisation control are applied to the information in question and the risk of possible unauthorised access is considered to be acceptable. The level of risk involved will be calculated by the Head of Assurance who will undertake a risk assessment of the third party or subcontractor prior to the granting of such access.

Where low risks are identified suitable action plans will be agreed between the Head of Assurance and the third party or subcontractor with clear dates set for the risks to be minimised or mitigated. Where risks of medium or above are identified these issues will be presented to the Information Security Forum where a clear course of action will be agreed. In some circumstances the Information Security Forum may (based on the level of risk) opt not to allow the service to commence and may seek alternative suppliers or subcontractors.

Depending on the results of the risk assessment third party or subcontractor information systems may require penetration testing. Such decisions will be taken by the Information Security Forum and any such testing will be managed and co-ordinated by the Head of Assurance.

Where subcontractors are to be granted direct access to company Information Systems the individual users will be trained in the use of the systems concerned. Such users will be subject to the same level of background checking as company employees. In addition subcontractors will be mandated to notify the company of leavers or role changes so access to such systems can be revoked in a timely manner.

All third parties and subcontractors will be made aware of their responsibility to report to the company any Information Security incidents. This should include the timeframes for reporting incidents and the process that will be followed.

Prior to sending any information to third parties or subcontractors, not only will the intended recipient be authorised to receive this information, but the procedures and Information Security measures adopted by the third party or subcontractor, will be

seen to continue to assure the confidentiality and integrity of the information to at least the same level applied within the company.

All external third parties and subcontractors who have access to company Information Assets will agree to follow the company Information Security policies. An appropriate summary of, or copy of, the relevant Information Security Policies will be formally delivered to any third party or subcontractor, prior to any such access being granted.

Non-disclosure agreements will be used in all situations between PeoplePlus and any third party or subcontractor, where the confidentiality, sensitivity or value of information being disclosed is classified as either Confidential or Sensitive. A non-disclosure agreement is a legal document between PeoplePlus and the third party which outlines confidential information which will be shared between one another but where access must be restricted. By signing up a non-disclosure agreement both parties agree not to disclose any information covered by the agreement. All potential suppliers will be required to sign up to a standard non-disclosure agreement before information is disclosed.

Where third parties are involved in providing critical services such as network infrastructure or public facing service, it is essential that they are able to meet the resilience and Information Security objectives of the service.

The Head of Assurance will ensure that third parties and subcontractors are subject to regular audits to ensure ongoing compliance with company policies and procedures.

Where the nature of the service provided by a third party or subcontractor is to be changed whether instigated by the third party/subcontractor or the company, all such changes will be subject to the company change control process.

12 Information security incident management

12.1 Incident Response Security Policy

Information Security incidents are all incidents that appear to breach PeoplePlus Information Security Policies and Procedures. It includes incidents where the security of corporate or personal data or PeoplePlus assets have been, or are believed to have been compromised, or where there have been any suspected security weaknesses or threats. All Information Security incidents must be reported immediately to the Head of Assurance.

An Information Security Hotline is available to report any incident. The Information Security Hotline number is **0800 032 1830**

PeoplePlus has adopted an open, honest and immediate reporting system to enable staff to report such incidents as effectively as possible. Unless incidents are responded to calmly, according to procedures - first to prevent the breach from continuing (if possible) and second, to inform the appropriate person(s) within the organisation – the business may incur both reputational and financial loss. In addition a failure to manage incidents could result in non-compliance with relevant legislation and contractual obligations.

All 3rd parties working with PeoplePlus should manage information security incident in accordance with this policy, tailored to reflect their internal structures and the nature of the information they hold, or create their own policy to a similar standard. The Information Security Hotline Number is available to all 3rd Parties to report an information security incident. If a 3rd party significantly changes their approach to Information Security the Head of Assurance should be notified.

12.1.1 Security Incidents

Within the company a security incident is an alert to the possibility that a breach of security may occur, be occurring or may have occurred.

A breach of security is where a stated company organisational policy or legal requirement regarding Information Security has been contravened. However, every incident, which suggests that the Confidentiality, Integrity or Availability of information has been inappropriately changed, can be considered a Security Incident. Every potential Security Breach will be initially treated as a Security Incident and only if confirmed does it become a Security Breach.

All Information Security Incidents within the company must be reported in accordance with the Information Security Incident Reporting Procedure. All Information Security incidents will be investigated and if appropriate a report and recommendations will be produced and if necessary the appropriate funding body

will be informed. It should be noted that individuals or groups of individuals who commit criminal acts involving company Information Assets will be prosecuted to the fullest extent of the law. Suitable procedures have been developed to ensure the appropriate collection and protection of evidence.

Software faults within systems used by the company must be formally recorded and reported to those responsible for software support / maintenance.

.All identified or suspected Information Security Weaknesses are to be notified immediately to the company's Head of Assurance.

A list of emergency contacts will be made available to relevant parties identified in the procedure.

12.1.2 Investigations and evidence

All company employees are to be made aware that evidence of Information Security incidents must be formally recorded, retained and brought to the attention of the Head of Assurance. .

Evidence relating to an Information Security Incident must be formally recorded and processed. Where appropriate dual control and segregation of duties will be incorporated into the procedures to ensure the integrity of such investigations.

Information Security incidents must be properly investigated by suitably trained and competent personnel. Staff must not attempt to undertake their own investigations.

Information Security incidents arising from system failures must be investigated by competent technicians.

The Head of Assurance must respond rapidly but calmly to all Information Security incidents, liaising and coordinating with colleagues to both gather information and offer advice. All Information Security incidents must be evaluated according to their particular circumstances, and this may, or may not, require various departments to be involved - ICT, Human Resources, Legal and Information Asset Owners. If it appears that disciplinary action against a member of staff is required, this must be handled in line with the company disciplinary procedures.

Information relating to Information Security incidents may only be released by authorised persons within the company or where contractually obliged.

A register of Information Security incidents and "lessons learned" must be maintained. The register should be studied regularly with any anecdotal evidence used to help reduce the risk and frequency of further Information Security incidents. All Information Security Incidents will be reported to the Information Security forum

The company must report Information Security incidents to relevant outside authorities, such as regulatory bodies, third party associates and law enforcement agencies, whenever this is required to comply with legal requirements or regulations or contractual obligations. This may only be done by authorised company personnel. The responsibility for making such reports lies with the company senior management.

13 Information Security Aspects of Business Continuity

13.1 Business Continuity Security Policy

To ensure that a Business Continuity Plan (BCP) is initiated, prepared, maintained and tested to provide critical key business services in the event of an unexpected occurrence which seriously disrupts the business. Should the need arise to trigger the BCP and it does not exist or is untested, is non-viable or fails when activated, then PeoplePlus (the company) may not be able to recover. The company Senior Management in conjunction with the Head of Assurance will prepare a Business Continuity Plan (BCP), including Emergency Response Plans. The detailed requirements for Business Continuity Plans will be driven from Business Impact Assessment and Risk Assessment exercises co-ordinated by the Head of Assurance.

The company Head of Assurance is responsible for preparation, maintenance and regular testing of business continuity plans to ensure that potential damage done by possible internal or external attacks can be minimised and that restoration takes place as quickly as possible. The BCP will be periodically tested to ensure that the management and staff understand how it is to be executed. All relevant company staff will be made aware of the BCP and their respective roles.

14 Compliance Security Policies

14.1 Compliance Security Policy

To ensure that PeoplePlus is compliant with applicable standards, regulation and legislation. Non-compliance may incur both reputation and financial loss to the business. All company employees will comply with the Information Security Policies of the organisation. Any Information Security incidents resulting from non-compliance may result in disciplinary action up to dismissal.

The company customer/client data and information will be classified at the appropriate level and secured accordingly. Client and staff information records are highly valuable to social engineers, fraudsters and identity thieves and will be considered as confidential or sensitive material.

Information held by the company relating to clients, staff, and third party contracts of the company is not for public consumption and will be protected and safeguarded from unauthorised access and disclosure.

The company intends to fully comply with the requirements of the following legislation:

- The Data Protection Act 1998
- The Computer Misuse Act 1990
- The Regulation of Investigatory Powers Act 2000
- Freedom of Information Act 2000
- The Copyright, Designs and Patents Act 1988
- Official Secrets Act 1989
- Human Rights Act 2000
- Retention of Records (Civil Evidence Act, Companies Act, Consumer Protection Act, Financial Services Act and Value Added Tax Act

<u>Data Protection Act 1998</u>

All PeoplePlus managers will adhere to guidelines to ensure that all employees are aware of the key aspects of the Data Protection Act 1998. PeoplePlus will only release personal and/or confidential information when required to do so by law or in the following circumstances:

- Where express permission is received from the person to whom the information relates.
- Where the information is already available to the public from other sources.
- Where it is not possible to identify any particular person from the information.
- When there is a serious risk of harm to the individual, for example, they are threatening suicide.

- To protect others. For example, information about possible or potential child abuse should be disclosed to the appropriate agency. Refer to the PeoplePlus Safeguarding Policy or contact one of our designated safeguarding officers.
- To prevent a serious criminal act, especially where others may be endangered, for example an act of terrorism.
- To assist with the investigation of a crime.

There is no obligation, in general, to pass on knowledge of a crime. However, it is a criminal offence to:

- Deliberately mislead the police.
- Receive a reward of any kind in return for not notifying the police about a criminal act.
- Fail to notify the police about an act that could be construed as an act of terrorism.
- Fail to notify the police about an act that could be construed as drug trafficking.

If data is released for any other reason than those stated above, it may be considered a breach of confidentiality and must be reported immediately to the Head of Assurance. Please refer to the Information Security Incident Policy for more details. Different operating business units may need to refer to, in addition, their own Operating Manuals.

Under the Data Protection Act 1998, it is possible for an individual to request any personal data PeoplePlus holds about them providing that proof of identity is supplied and upon payment of a fee, where levied. The request is known as a Subject Access Request.

Any such requests must be made in writing and forwarded to appropriate department. Requests will be responded to within the statutory timeframes.

Computer Misuse Act 1990

All PeoplePlus managers will adhere to guidelines to ensure that all employees are aware of the key aspects of Computer Misuse legislation in so far as these requirements impact on their duties.

Regulation of Investigatory Powers Act 2000

Under the Regulation of Investigatory Powers Act (2000) PeoplePlus reserve the right to monitor traffic transmitted over its networks or data stored on its PCs or servers. This act also means that in the event of a breach of national security the Government may also be given information relating to personal documents or emails. Similarly the police may be given access to information contained within our files or transmitted on our network for the purposes of preventing or investigating crime.

Freedom of Information Action 2000

The Freedom of Information Act 2000 (FOIA) gives any person, acting singularly or as a member of an organisation, the legal right to gain information relevant to a public body's dealings, whether they are contractual or non-contractual and would relate to PeoplePlus in its business dealings with such public bodies. Please refer to the Freedom of Information Policy for further information.

Copyright, Designs and Patents Act 1988

Information from the Internet or other electronic sources may not be used within the company without authorisation from the owner of the copyright. Company managers will adhere to guidelines to ensure that all employees are aware of the key aspects of Software Copyright and licensing legislation, in so far as these requirements impact on their duties.

Official Secrets Act 1989

Under the Official Secrets Act 1989, it is an offence to disclosure official information including information received from the DWP or other government departments which may be damaging to the national interest. The Official Secrets Act 1989 applies to all employees and to all members of the public who possess or have access to official information. Section 8 of the Official Secrets Act 1989 requires that anyone who is entrusted with sensitive documents or articles (for example, personal information, sensitive reports etc), takes care to prevent unauthorised disclosure and to deal with them in a manner specified in their official job role/duties

The 'need to know' principle is fundamental to the protection of sensitive government and PeoplePlus assets. Their distribution should be limited to those with authorised access and should be no wider than is necessary for the secure and efficient conduct of PeoplePlus business. Access should be denied to any individual who does not need access to a specific protectively marked asset irrespective of their level of access or clearance.

The Official Secrets Act is associated with and assists in compliance with European Convention on Human Rights (ECHR), Data Protection Act 1998, Health and Safety at Work etc Act 1974 and Crime and Disorder Act 1998

14.2 Records Management Policy

To ensure that all records within PeoplePlus (the company) are protected from loss, destruction and falsification in accordance with statutory, regulatory, contractual and business requirements the provisions of this policy must followed.

Records are defined as all those documents, which facilitate the business carried out by the company (to provide services to customers and clients) and which are

thereafter retained (for a set period) or are used in the day to day running of the company. These records may be created, received or maintained in hard copy or electronic format.

This policy applies to all records created, received or maintained by staff of the company in the course of carrying out their daily duties.

Records management is defined as a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of, and information about, business activities and transactions.

The company has a corporate responsibility to maintain its records and recordkeeping systems in accordance with the regulatory environment. The role with overall responsibility for this sits with the Commercial Director.

The Commercial Director is responsible for drawing up guidance for good records management practice and promoting compliance in such a way as to ensure the easy, appropriate and timely retrieval of information.

Individual employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the company's records management guidelines.

The destruction of records will only take place when authorised by the Commercial Director in line with the requirements of the Disposal and Decommissioning Policy Security Policy contained within Section 6.3.

Guidance on the procedures necessary to comply with this Policy is available from the Head of Quality and Curriculum. This guidance covers:

- Records creation
- Business classification (for filing schemes)
- Retention periods for records
- Storage options for records
- Destruction options for records
- Archival records: selection and management
- External codes of practice and relevant legislation

15 Other Policies

15.1 Remote/Mobile Computing Policy

For the purposes of this policy the term “remote/mobile worker” applies to all individuals using PeoplePlus supplied mobile IT devices (i.e. laptops/notebooks/smartphone etc.) beyond the Company’s physical perimeter (i.e. premises) in the performance of their role and those authorised to work at alternative sites or from home on a permanent or regular basis. Remote/Mobile workers must use PeoplePlus equipment. Remote/Mobile Workers are not permitted to use any personal PC’s or Laptops, Data Storage Devices (external hard drives, USB memory sticks or personal email accounts to carry out any PeoplePlus business.

The authority to work remotely and/or within the mobile environment is granted by an employee's organisational line manager who must be satisfied that the employee’s role can be effectively performed off-site, as required, before a remote/mobile working arrangement can commence. The line manager must be confident that the employee has the personality and work habits suitable for remote/mobile working, and that any permanent alternative work site is appropriate for the conduct of PeoplePlus business operations. Any considerations for permanent/regular alternative sites should address physical and information security aspects of PeoplePlus and partner business information, associated assets and property.

Remote/mobile workers and line managers must ensure that PeoplePlus security standards are applied to remote/mobile working environments wherever possible to ensure PeoplePlus information and information assets are not put at risk from loss or compromise. Where this cannot be achieved, alternative measures must be applied and the alternative measures must be subject to appropriate risk assessment and management by the Head of Assurance and approved by the Information Security Forum and/or Senior Management Team. In practice this means that employees must protect information in a similar manner no matter whether they are in an PeoplePlus office, a hotel room, or working at home.

The PeoplePlus Clear Desk and Screen Policy detailed in Section 3.1 applies to remote/mobile workers and remote/alternate work sites. Employees must ensure that display screens for all remote/mobile systems are positioned in a manner such that they cannot be readily viewed by unauthorised persons through a window, over a shoulder, or by similar means. Remote/mobile workers must not share passwords, tokens, smart cards or other access devices with others. If appropriate, privacy filters should be used. Remote/mobile computing devices supplied for processing of PeoplePlus business information are provided for the exclusive use of the employee. They must not be used by, or loaned to, family members, friends or others.

Mobile devices (e.g. laptop, PDA, mobile phone, smart phone etc.) should not be left unattended when not in use. Employees should pay particular attention to the safe custody of mobile devices during travel (airports, trains, hotels, baggage scans etc.). Mobile computing devices (laptop, netbooks etc.) are not to be left in standby/hibernation mode during travel and they are not to be left in cars.

When using mobile phones employees should also be wary of being overheard when discussing PeoplePlus or other company business over mobile phones, particularly in public places and should use guarded terms and refrain from mentioning detail beyond that needed to get the job done.

Mobile phones, smart phones, PDA/handheld computers etc. (other than Company supplied BlackBerry /smart phones) must not be used to store PeoplePlus business information. Exceptions will be made for calendars, address books, and stored connection information such as telephone numbers. However, they should not to be used to store confidential information on a regular basis; such information should be stored on network file servers. Mobile phones and smart phones are to be protected by password/pin number.

All computers issued to PeoplePlus employees and/or associates used for remote/mobile working (desktop PCs, laptops, netbooks etc) must be protected by a Company approved hard disk encryption application with boot protection supplied and installed by ICT Department. Such products generally protect the contents of computers when the data is at rest (i.e. when they are shut down). They do not generally protect contents after boot-up (i.e. when operating), except where files are individually encrypted. Consequently, remote/mobile computers are not to be left unattended in hibernate/standby mode and they must not be left in hibernate/standby mode during travel.

Remote/mobile workers must connect to the Company network via PeoplePlus Secure Client VPN. PeoplePlus remote access authentication credentials are not be shared or given to any other person, including line managers. This is essential for the security of the Company network so that the system is able to identify users, and their associated devices, and to validate that identity to ensure they are authentic and accountable. Once this authentication has been carried out, controls within the system will ensure users are only able to access systems, data or services for which they have been authorised. Employees must not leave laptops/netbooks/terminals unattended during remote SecureClient VPN or SSL web-mail sessions nor establish any other communications systems that ordinarily accept in-coming dial-up calls or connections.

Company Remote/mobile workers must use only Company-provided computer software, hardware, and network equipment. Company Partners, contractors, consultants and other third parties with remote access privileges must only connect to the Company network using business-owned computing devices approved by ICT Department in line with company policies. All computing devices connecting to the company network remotely, by any means, will have a fully operational personal firewall and an up-to-date anti-malware application installed or approved by ICT Department.

Personally-owned computing devices are not permitted to connect to the Company network and systems, or be used in any other way to process or otherwise handle PeoplePlus business information.

Remote/mobile computers internal clocks are to be kept synchronized to actual/network date and time (this can be achieved through regular connection to the PeoplePlus network).

Employees must not change operating system configuration, disable any computer services or install new software on Company-supplied computer hardware without permission from

ICT Department. Computer equipment supplied by PeoplePlus must not be altered or added to in any way. If such changes are required, they must be approved by ICT Department and be performed by ICT Department personnel on-site or with remote system maintenance software.

Employees must not download software from the Internet, or other external systems/sources beyond the PeoplePlus Network onto Company-provided Computers without the prior approval of ICT Department.

Remote/mobile workers are responsible for ensuring that their mobile systems and devices are backed up on a periodic basis, automatically through the network if network backup is not available or feasible, ICT Department will provide remote workers with the appropriate equipment. If these backups contain confidential information, the backups must be encrypted using an encryption solution approved and provided by ICT Department.

Confidential information is to be stored on-line on appropriate Company network fileservers and is not to be written to removable media without the express authority of line management.

Employees must receive remote systems access training prior to being granted privileges to use in-bound VPN, or any other PeoplePlus remote access data communications system.

Employees who have a business requirement to retain or store confidential PeoplePlus business information at their homes, or other alternative site, and have the authority of their departmental manager and the Head of Assurance to do so, must be provided with appropriate secure lockable furniture and/or ICT Department approved encryption solutions for the secure storage of such information.

Remote/mobile workers authorised to work permanently or regularly from home or other alternative site are to be provided with an appropriate means to dispose of waste hard-copy confidential business information. All PeoplePlus paper-resident confidential business information must be destroyed by CROSS-CUT shredder or other approved and contracted confidential waste disposal service. Remote/mobile workers must not dispose of confidential PeoplePlus business information in hotel wastebaskets or other publicly-accessible waste containers. Confidential business information is to be retained until it can be cross-cut shredded, or destroyed by other approved methods.

When PeoplePlus supplies a remote/mobile worker with software, hardware, information or other materials (e.g. furniture) to conduct PeoplePlus business remotely, the title and all rights and interests to these items will remain with the PeoplePlus. In such instances, remote/mobile worker possession does not convey ownership or any implication of ownership. All such items must be promptly returned to the Company when a remote/mobile worker's employment or other association with PeoplePlus ceases, or when so requested by the employees' line manager or ICT Department.

When PeoplePlus supplies a remote/mobile worker with software, hardware, information or other materials to perform PeoplePlus business remotely, PeoplePlus assumes all risks of loss or damage to these items unless such loss or damage occurs due to the remote/mobile worker's negligence or failure to comply with Company policy. PeoplePlus expressly

disclaims any responsibility for loss or damage to persons or property caused by, or arising out of the usage of such items.

PeoplePlus maintains the right to conduct physical inspections of remote/mobile worker's permanent or regular alternative sites without advance notice. PeoplePlus maintains the right to examine the contents of computers used by employees, contractors, consultants, third parties and other temporary staff, which are authorised by ICT Department to connect to the PeoplePlus Network and to process PeoplePlus business information, including the right to remotely inspect the contents of, and configuration of, computers used by remote/mobile workers through remote systems administration tools.

If remote/mobile workers are required to use equipment on a non-PeoplePlus internet connection such a home internet, on a train or in a managed office ensure that you only use trusted sources.

Encrypted devices or encryption software must not be taken outside the UK without prior discussion and agreement with the Head of Assurance. This is because certain countries have specific legislation which does not permit the import of certain encryption types.

Remote/mobile workers must immediately report any loss, damage or compromise of PeoplePlus remote/mobile computer hardware, mobile phones, smart phones, software or business information entrusted to their care to the Head of Assurance via the Security Incident Hotline (0800 032 1830). PeoplePlus reserves the right to check any equipment provided to remote/mobile workers at any time and where necessary withdraw access.

15.2 Data Protection, Copyright & Confidentiality Policy

Data Protection
The PeoplePlus is registered with the Information Commissioner for the purposes of the Data protection Act.

The Group takes data protection very seriously and as such complies with the eight principles of the act. In broad terms the act states that personal data shall: -

- be obtained and processed fairly and lawfully.
- be held only for lawful purposes, which are described in the register entry.
- be used or disclosed only for those or compatible purposes.
- be adequate, relevant and not excessive in relation to the purpose for which they are held.
- be accurate and where necessary, kept up to date.
- be held no longer than is necessary for the purpose for which they are held.
- be surrounded by proper security.

Personal data held by the organisation includes data for staff and customers. This data is held electronically and also in hard copy in PeoplePlus locations.

At location level, access to hard copy information is restricted, as this information is retained in suitable storage mediums away from general areas. Access to this information is restricted to only those who have a legitimate requirement to use / view the information.

Wherever, information is held, appropriate safeguards are in place to prevent unauthorised use/disclosure of the data. Hard copies are retained in suitable secure storage mediums

with restricted access. Data held on electronic media have security protocols built into the system, such as individual access codes, which are password protected. Any disclosure of information is within the terms specified of the organisations registration with the Information Commissioner for data protection.

Copyright

All written material provided to employees or produced by employees during employment with PeoplePlus, whether hard copy - paper, electronic or magnetic – computers, disks or CDs,is the sole property of PeoplePlus (who own the copyright of all contents). This information is made available for use by the staff of the PeoplePlus, and those of its authorised contract associates. The time of termination of your employment with us, or at any other time upon demand, you shall return to us any such material in your possession.

Confidentiality

PeoplePlus is committed to ensuring the confidentiality of all information. To achieve this, we have policies, procedures and a system in place confidentiality is maintained at all times.

a) All information that: -

- Is or has been acquired by staff during, or in the course of their employment, or has otherwise been acquired in confidence.
- Relates particularly to the organisations' business, or that of other persons or bodies with whom we have dealings of any sort, and
- Has not been made public by, or with our authority,

Shall be confidential and (Save in the course of our business or as required by law) you shall not at any time, whether before or after the termination of your employment, disclose such information to any person without our written consent. This includes any confidential information or trade secrets concerning the business or finances, designs, processes, dealings, transactions or affairs

b) All staff are to exercise reasonable care to keep safe all documentary or other material containing confidential information, in line with the requirements of data protection and shall at the time of termination of their employment with us, or at any other time upon demand, return to us any such material in their possession.

Case/383612

SERVICES CONTRACT

-between-

(1) THE SCOTTISH MINISTERS (THE "PURCHASER")

-and-

(2) PEOPLEPLUS GROUP LIMITED (THE "SERVICE PROVIDER")

-relating to the supply of-

FAIR START SCOTLAND EMPLOYABILITY SUPPORT SERVICES 2018

LOT 8 – HIGHLANDS AND ISLANDS (ARGYLL AND BUTE, EILEAN SIAR, HIGHLAND, MORAY, ORKNEY ISLANDS AND SHETLAND ISLANDS)

Table of Contents

SECTION A INTRODUCTORY PROVISIONS

1. Definitions and Interpretation
2. Condition Precedent
3. Nature of the Contract
4. Period
5. Break
5A. Implementation
6. Specification and Service Levels
7. Pricing Schedule
8. Management Arrangements

SECTION B MISCELLANEOUS PROVISIONS INCLUDING THOSE RELATING TO PRICE, PAYMENT AND INFORMATION

9. Service Provider's Status
10. Notices
11. Price
12. Payment and Invoicing
13. Recovery of Sums Due
14. Data Protection Act
15. Freedom of Information
16. Purchaser Protected Information
17. Service Provider Sensitive Information
18. Audit and Records Management
19. Publicity

SECTION C PROVISION OF SERVICES

20. Provision of the Services
21. Deliverables and Milestones
21A. Assurance and Fraud Reviews

SECTION D STAFF INVOLVED IN THE PROVISION OF SERVICES

22. Key Individuals
23. Offers of Employment
24. Staff transfer at commencement
25. Information about Service Provider Employees
26. Staff transfer on expiry or termination
27. Security

SECTION E PROVISIONS RELATING TO INTELLECTUAL PROPERTY AND GOVERNANCE

28. Parties' pre-existing Intellectual Property Rights
29. Specially Created Intellectual Property Rights
30. Licenses of Intellectual Property Rights
31. Claims relating to Intellectual Property Rights
32. Assignation
33. Change of Control
34. Sub-Contracting
35. Amendment

SECTION F SERVICE PROVIDER CONDUCT REQUIREMENTS

36. Compliance with the Law etc.
37. Official Secrets Acts
38. Service Provider's responsibility for staff etc.
39. Access to the Purchaser's premises
40. Service Provider's Equipment
41. Purchaser Property
42. Health and Safety etc.
42A. Effective Procedures
43. Offences
44. Tax arrangements
45. Discrimination
46. Blacklisting
47. Sustainability etc.
48. Conflicts of Interest

SECTION G FINAL PROVISIONS

49. Warranties and Representations
50. General Indemnity
51. Limitation of Liability
52. Insurances
53. Force Majeure
54. Dispute Resolution
55. Severability
56. Waiver and Cumulative Remedies
57. Termination Rights
58. Termination on Insolvency or Change of Control
59. Exit Management
60. Consequences of Expiry or Termination
61. Entire Agreement
62. Governing Law and Jurisdiction

SCHEDULES

Schedule 1 Specification and Service Levels
Schedule 2 Pricing Schedule
Schedule 3 Change Control Procedures
Schedule 4 Management Arrangements
Schedule 5 Key Individuals
Schedule 6 Approved Sub-contractors
Schedule 7 Service Provider Sensitive Information
Schedule 8 Parent Company Guarantee – NOT USED
Schedule 9 Model Contract regarding Data Protection Directive 95/46/EC
Schedule 10 Exit Management
Schedule 11 Business Continuity and Disaster Recovery (BCDR)
Schedule 12 Security
Schedule 13 Implementation Plan

PREAMBLE:

ONE The Purchaser requires the provision of services;

TWO On 9th March 2017 the Purchaser's contract notice relating to the Services was published in the Official Journal of the European Union with reference number 2017/S 048-088157;

THREE Not Used;

FOUR On 9 March 2017 the Purchaser issued its ITT to potential Service Providers (including the Service Provider) in respect of the provision of services;

FIVE On 23rd May 2017 the Service Provider submitted its Tender;

SIX On the basis of the Tender, the Purchaser has selected the Service Provider to supply the Services under the Contract;

SEVEN The Contract establishes standard terms of supply for the provision of services;

EIGHT The Contract also includes:

- a Specification setting out the Services that the Service Provider has undertaken to provide including Service Levels setting out particular levels of service that the Service Provider has undertaken to meet;
- a Pricing Schedule setting out details of the pricing of the Services, including provision for Service Credits;
- details of Key Individuals involved in the provision of the Services;
- details of approved sub-contractors as at Contract award;
- details of the Service Provider's information which is deemed to be Service Provider Sensitive Information;
- Management Arrangements for the strategic management of the relationship between the Parties.

SUBSTANTIVE PROVISIONS:

SECTION A: INTRODUCTORY PROVISIONS

1. Definitions and Interpretation

1.1. In the Contract, unless the context otherwise requires, the following terms have the meanings given to them below:

"Access to Work (AtW)" Access to Work is a Department for Work and Pensions service that provides practical advice and support to disabled people and their employers to help overcome work related obstacles resulting from disability. The service also provides grants towards additional work-related support relating to a person's disability.

"**Achieve**" or "**Achievement**" means meeting the criteria for the achievement or satisfaction of a Milestone, as set out in the Implementation Plan.

"**Approval**" means the written consent of the Purchaser.

"**Assignee**" has the meaning given in clause 32.2 (Assignation).

"Balance of time" means the remaining period that a Customer can expect to receive pre-employment and in-work support should they disengage from the Service.

"Baseline Personnel Security Standard" means the pre-employment controls for all civil servants, members of the Armed Forces, temporary staff and government contractors generally.

"BCDR Plan" means the business continuity and disaster recovery plan set out in Schedule 11 (Business Continuity and Disaster Recovery (BCDR)), as may be amended from time to time.

"Better off in Work Calculation" means a better off calculation that produces accurate estimates of how much better off a Customer could be in work based on information supplied by the Customer, of potential in-work benefits and tax credits.

"Branding" means all names, logos, images, designs and marks of the Purchaser associated with the Programme and the relevant website domain names including, without limitation, those domain names listed in Schedule 1 (Specification and Service Levels).

"Case Conferencing" means a formal, planned, and structured event separate from regular contacts. The goal of case conferencing is to provide holistic, coordinated, and integrated services across organisations, and to reduce duplication, to best support the Customer.

"Change" means as defined in paragraph 1.1 of Schedule 3 (Change Control Procedures).

"Change Control Notice" or "CCN" a written response or request made by either the Service Provider or the Purchaser in accordance with the Change Control Procedure,

"Change Control Procedures" means the change control procedure specified in Schedule 3 – Change Control Procedures.

"**Change in Law**" means any change in Law which impacts on the performance of the Services which comes into force after the Effective Date.

"Community Benefits" means benefits for society or the environment.

"Continuous Improvement Strategy" means a strategy for improving the provision of

the Services which is produced by the Service Provider.

"**Contract**" means this Contract between the Parties consisting of clauses and thirteen Schedules.

"Contract Charges" means the prices (inclusive of any Milestone Payments, licence costs, support and maintenance costs, exclusive of any applicable VAT), payable to the Service Provider by the Purchaser under this Contract, as set out in the Pricing Schedule, for the full and proper performance by the Service Provider of its obligations under this Contract.

"Contract Period" means the term of the Contract as defined in clause 4.1 provided that such term shall be extended where applicable in accordance with clause 4.2 and shall also include any additional periods of time as required in respect of clauses 4.3 (if applicable) and 4.4 (if applicable) (subject to any earlier date where the Contract is terminated in accordance with the terms of the Contract).

"Contract Review Report" refers to a monthly report on service delivery performance, at a Lot level highlighting issues, risks and best practice.

"Contract Year" shall mean the 12 month period commencing on the Effective Date or any anniversary thereof.

"**Contracting Authority**" has the meaning given in regulation 2 of the Public Contracts (Scotland) Regulations 2015;

"**Control**" has the meaning given in section 450 of the Corporation Tax Act 2010.

"**Core Hours**" means an hour between 0900 hours and 1700 hours on a Working Day.

"Customer" means any individual to whom the Service Provider provides support pursuant to the Contract.

"Customer Charter" means the document which details the Service Provider's values and principles and which includes a description of the guaranteed standards of service to be provided to Customers, how the Services will be delivered to those Customers and what the expected outcomes are from a Customer's perspective.

"Data Sharing Protocol" means the data sharing protocol entered into between the Service Provider and the Purchaser with relevant third parties in relation to the Services (e.g. the Department for Work and Pensions, and/or the Partner Organisations) annexed to Schedule 9 (Model Contract regarding Data Protection Directive 95/46/EC).

"**Default**" means any breach of the obligations of a Party under the Contract (including material breach) or any negligent act, omission or statement of a Party in connection with or in relation to the Contract.

"Delay" means:

(a) a delay in the Achievement of a Milestone by its Milestone Date; or

(b) a delay in the design, development, testing or implementation of a Deliverable by the relevant date set out in the Implementation Plan;

"**Deliverable**" means an item, feature or service associated with the provision of the Services which is required to be delivered by the Service Provider at a Milestone Date or at any other stage during the performance of the Contract.

"**Detailed Implementation Plan**" means the detailed plan for the implementation of the Services which is developed in accordance with paragraph 41 (Mobilisation and Implementation) Schedule 1 (Specification and Service Levels).

"Disabled Customers" means people defined as disabled by the Equalities Act 2010 and in need of the specialist support that is only available in the Intense or Advanced strands of the Scottish Employability Programme.

"Documentation" means all documentation as:

(a) is required to be supplied by the Service Provider to the Purchaser under this Contract;

(b) would reasonably be required by a competent third party contracted by the Purchaser to provide the Services in accordance with Good Industry Practice;

(c) is required by the Service Provider in order to provide the Services; and/or

(d) has or will be generated for the purpose of providing the Services.

"Effective Date" means the date which this Contract is signed by both Parties. (October 2017)

"Employment and Support Allowance"(ESA) means the integrated contributory and income-based benefit, which replaced Incapacity Benefit and Income Support, paid on the grounds of incapacity for most new and repeat customers from October 2008. ESA is paid to those who have limited capability for work (i.e. the customer's physical or mental condition limits their capability to work such that it is not reasonable to require them to work). An ESA customer in the work related activity group must undertake work focused interviews, participate in work related activity and agree an action plan.

"Employment and Support Allowance Work Related Activity Group" means following a Work Capability Assessment DWP will place Customers in either the work-related activity group (WRAG) or support group if they are entitled to ESA. DWP expect Customers in the WRAG to attend regular interviews with an advisor who can help with things like job goals and improving skills.

"**Environmental Information Regulations**" means the Environmental Information (Scotland) Regulations 2004 (and any subordinate regulations made under them from time to time or any superseding or amending regulations) together with any guidance and/or codes or practice issued by the Information Commissioner, the Scottish Information Commissioner and/or any relevant government department in relation to such regulations.

"**ESPD**" means the European Single Procurement Document completed by the Contractor and sent to the Authority on 23rd May 2017.

"**Equipment**" means equipment, computer systems, (including hardware, software and peripherals plant, tackle, materials and other items supplied and used by the Service Provider's Representatives in the performance of the Service Provider's obligations under the Contract.

"**Exit Management**" means the obligations and rights of the Parties to ensure a smooth transition of the Contract from the Service Provider to the Purchaser or any Replacement Service Provider as set out in Clause 59 (Exit Management) and Schedule 10 (Exit Management).

"**Exit Plan**" means the exit plan to be developed and updated by the Service Provider in accordance with Schedule 10 (Exit Management).

"Experience Panel" means the Scottish Government are setting up a series of Experience Panels to gather feedback on the roll-out of devolved Benefits across

Scotland. A specific Experience Panel for Employability Services is being developed. There will be a choice of activities e.g. short surveys, interviews, discussion groups and these may be carried out face-to-face, by phone or online. All materials relating to the Experience Panel recruitment and activity will be provided by The Scottish Government.

"**FOISA**" means the Freedom of Information (Scotland) Act 2002 and any subordinate legislation made under this Act from time to time or any superseding or amending enactments or regulations, together with any guidance and/or codes of practice issued by the Information Commissioner, the Scottish Information Commissioner and/or any relevant government department in relation to such legislation.

"**Force Majeure**" means any event or occurrence which is outside the reasonable control of the Party concerned and which is not attributable to any act or failure to take preventative action by that Party, including industrial action, fire, flood, violent storm, pestilence, explosion, malicious damage, armed conflict, acts of terrorism, nuclear, biological or chemical warfare, or any other disaster, natural or man-made.

"**Good Industry Practice**" means standards, practices, methods and procedures conforming to legal and regulatory requirements and the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar type of undertaking as the Service Provider under the same or similar circumstances.

"**Go Live Services**" means the service delivery go live (i.e. Customer start) services to be performed by the Service Provider as outlined in Schedule 1 (Specification and Service Levels).

"Government Gateway" means a secure authentication route into Government IT services.

"Guaranteed Service Standards" means the minimum level of support all Customers accessing the Service must receive regardless of who they are and where they live. The guarantee will include the frequency of meetings and interventions with customers, the development of a tailored action plan and the support they will receive to remain in work when they get a job.

"**Implementation Plan**" means the Initial Implementation Plan until it is superseded by the Detailed Implementation Plan (as subsequently updated in accordance with paragraph 40 (Mobilisation and Implementation) of Schedule 1 (Specification and Service Levels).

"**Incoming Employees**" means individuals whose employment transfers to the Service Provider on the commencement of the provision of the Services by operation of TUPE.

"Individual Placement and Support" or ""**IPS**" means a supported employment model that works with people diagnosed with severe and enduring mental illness to help them find sustainable, competitive jobs in the community that fits their needs and interests. A key principle of IPS is that employment specialists and clinical teams work together to support people to gain employment. Other principles of IPS match the principles of supported employment, as laid out in the Supported Employment Framework for Scotland - for instance, it provides vocational profiling, job finding and employer Engagement as well as person-centred on and off the job support and aftercare. Often the job search part of the process can be much more rapid in IPS than in the traditional supported employment model.

"**Initial Implementation Plan**" means the document entitled Implementation Plan as set out in Schedule 13 (Implementation Plan).

"**Initial Referral Period**" has the meaning set out in clause 4.1.1.

"**Intellectual Property Rights**" means patents, inventions, trade marks, service marks, logos, design rights (whether registerable or otherwise), applications for any of the foregoing, copyright, database rights, domain names, trade or business names, moral rights and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom) and the right to sue for passing off.

"Intermediate Labour Market (ILM)" means a model of waged work in specially created temporary jobs.

"**ITT**" means the Purchaser's invitation to tender dated 9th March 2017.

"**JCP**" or "**Jobcentre Plus**" means Jobcentre Plus being a government-funded employment agency and social security office, whose aim it is to help people of working age find employment in the UK.

"Job Analysis" means once a suitable job is identified for a Customer, a job analysis can be undertaken. This checks any assumptions made in the job description and thoroughly investigates the job on offer so that all elements of the job and the work place are understood. This can include job duties, hours and days of work, health and safety considerations, accessibility, and workplace culture. The job analysis might point towards ways of carving parts of job descriptions that suit the workers' talents, or creating new job descriptions that suit the worker and are cost effective for the employer.

"Jobseekers Allowance" an allowance payable to Customers who are out of work, or working less than 16 hours a week, are aged under pension age and are actively seeking and capable of work.

"**Job Outcome**" means the outcomes as detailed in the first Key Performance Indicator in Annex E to Schedule 1 (Specification and Service Levels).

"**Judicial Order**" means an ineffectiveness order or an order shortening the duration of the contract made in relation to the Contract under Chapter 6 of the Public Contracts (Scotland) Regulations 2015.

"**Key Individuals**" means the Service Provider Representatives identified as being key individuals for the provision of the Services as set out in Schedule 5 (Key Individuals).

"**Key Delivery Indicator**" or "**KDI**" means the key delivery indicators as outlined in Annex F to Schedule 1 (Specification and Service Levels).

"**Key Performance Indicator**" or "**KPI**" means the key performance indicators as outlined in Annex E to Schedule 1 (Specification and Service Levels).

"KPI Failure" means a failure to meet the minimum performance expectations (or any higher standard outlined in Annex 2 of the Pricing Schedule, where relevant) in respect of the KPIs.

"**Law**" means any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972, regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Service Provider is bound to comply.

"Lot" means the geographical footprint for the specified geographical area in Scotland as set out in Annex C of Schedule 1 (Specification and Service Levels).

"**Management Arrangements**" means the arrangements for the strategic management of the relationship between the Parties, including arrangements for monitoring of the Service Provider's compliance with the Specification, the Service Levels, and the terms of the Contract, set out in Schedule 4 (Management Arranagements).

"**Milestone**" means any event or task which must be completed by a particular date, such as the delivery of a Deliverable, identified as a Milestone in accordance with the the Implementation Plan.

"Milestone Date" means the target date set out against the relevant Milestone in the Implementation Plan by which the Achievement of the Milestone must have been met;

"Milestone Payment" means a payment identified in the Implementation Plan to be made following the Achievement of the relevant Milestone.

"Operational Guidance" means detailed guidance and information (including processes) which is provided by the Scottish Government to the Service Provider to use when delivering the Services.

"**Operational Services**" means any and all of the operational services to be performed by the Service Provider that commence from the first customer referral activity as outlined in Schedule 1 (Specification and Service Levels).

"**Outcomes**" means the Job Outcomes and Sustained Job Outcomes as outlined in Annex E to Schedule 1 (Specification and Service Levels).

"**Outgoing Employees**" means individuals whose employment transfers from the Service Provider on the ceasing of the provision of the Services by the Service Provider by operation of TUPE.

"Parent Company" means any company which is the ultimate Holding Company of the Service Provider and which is either responsible directly or indirectly for the business activities of the Service Provider or which is engaged by the same or similar business to the Service Provider. The term Holding or Parent Company shall have the meaning ascribed by the Companies Act 2006 or any statutory re-enactment or amendment thereto.

"Participation Agreement" means a signed, joint agreement which sets out the commitments of the Service Provider and Customer, and which outlines the service offer and roles and responsibilities for each party.

"Partner Organisation" means the wide range of organisations that support or provide services of potential use to Customers.

"**Party**" means either of the Purchaser or the Service Provider.

"PRaP" means the Provider Referrals and Payments system which enables secure, automated exchanges of information about customers referred to providers, and payments from DWP to Prime Providers. Providers access PRaP securely through the Government Gateway. The PRaP system also provides data about the cost and performance of contracted provision, supporting contract and performance management.

"**Pricing Schedule**" means the details of the pricing of the Services including provision for Service Credits, set out in Schedule 2.

"**Programme**" means the Fair Start Scotland scheme outlined in Schedule 1 (Specification and Service Levels).

"**Purchaser**" means the Scottish Ministers.

"Purchaser Contract Manager" means the individual within the Purchaser's organisation responsible for the day to day management of the Contract.

"**Purchaser Data**" means as defined in Schedule 10 (Exit Management).

"**Purchaser Property**" means any corporeal moveable property issued or made available to the Service Provider by the Purchaser in connection with the Contract.

"**Purchaser Protected Information**" means any information provided by the Purchaser to the Service Provider which:

- carries a protective marking such as "Official", "Secret" or "Top Secret"; or
- is exempt information as set out in Part 2 of FOISA (disregarding for that purpose whether a provision of Part 2 does not confer absolute exemption within the meaning of section 2(2) of FOISA).

"Referral Agency" means any organisation, for example, Jobcentre Plus, Third Sector; Social Service Teams; Carer Groups; Education and Learning institutions, NHS; and Local Authorities that supports a Customer to participate in the Service through a referral to the Service Provider.

"**Referral Period**" means as defined in clause 4.1.1.

"**Relevant Transfer**" has the meaning given in regulation 2(1) of TUPE.

"**Replacement Service Provider**" means any third party service provider appointed to perform the Services by the Purchaser from time to time.

"Retention" means support for employees (or a self-employed people) who become newly disabled, or their existing disability changes in a way that puts their prospects of continued employment at serious risk, to retain current employment. Retention provision via the Programme may extend to Customers who have not been supported by the Service Provider for pre-employment support.

"**Request for Information**" means a request for information within the meaning of section 8 of FOISA or the Environmental Information Regulations and any attempted or apparent such request.

"Scottish Government Performance Management and Operations Support Team" means the team responsible for the day to day contract management of the Contract, their main function is to provide support to the Service Provider and Referral Agencies on administration and performance management of the Programme.

"**Schedule**" means a schedule annexed to, and forming part of, the Contract.

"**Self-employment**" or "**self-employment**" means where the Customer is trading independently for a period of time as defined in the Outcomes.

"**Services**" means any and all of the Services to be supplied by the Service Provider to the Purchaser under the Contract including those set out in the Specification.

"**Service Credits**" means the service credits payable to the Purchaser by the Service Provider in the event that the Service Levels are not met and identified as service credits in the Pricing Schedule.

"**Service Levels**" means the Key Performance Indicators and the Key Delivery Indicators identified as such in the Specification.

"Service Commencement Date" means the date of first Customer Referral activity (i.e. start of operational services 13th March 2018).

"**Services Go-Live Commencement Date**" means the date of the Go Live Customer Service date (3rd April 2018).

"**Service Provider**" means PeoplePlus Group Limited.

"Service Provider Contract Manager" means the individual within the Service Proivder's organisation responsible for the day to day management of the Contract.

"**Service Provider Representatives**" means all persons engaged by the Service Provider in the performance of its obligations under the Contract including:

- its employees and workers (including persons employed by a third party but working for and under the control of the Service Provider);
- its agents, Service Providers and carriers;
- any sub-contractors of the Service Provider (whether approved under clause 34 (Sub-contracting) or otherwise); and
- any other third parties used by the Service Provider in performing the Services or any third parties that the Service Provider refers Customers to as part of the Services.

"**Service Provider Sensitive Information**" means any information provided by the Service Provider to the Purchaser (disregarding any protective marking or assertion of confidentiality) which:

- is specified as Service Provider Sensitive Information in Schedule 7 and has not lost its sensitivity according to the justifications and durations set out in that Schedule; and
- is exempt information pursuant to sections 33(1) or 36, 38 or 39 of FOISA (having regard for that purpose to the public interest there might be in disclosing such information as referred to in section 2(1)(b) of FOISA).

"**Service Provider System**" means the IT components of the system(s) operated by the Service Provider to perform the Services, including all hardware, infrastructure, platforms and software, application platforms and software, database management platforms and data, and third-party software.

"**Service Transfer Date**" means the date on which the Services (or any part of the Services), for whatever reason transfer from the Service Provider to the Purchaser or any Replacement Service Provider.

"**Sites"** means:

(a) any premises (including the Purchaser's premises, the Service Provider's premises or third party premises):

(i) from, to or at which:
(1) the Services are (or are to be) provided; or
(2) the Service Provider manages, organises or otherwise directs the provision or the use of the Services; or

(ii) where: any part of the Service Provider System is situated; or b) any physical interface with the Purchaser's IT system or PRaP takes place.

"SME" means small to medium-sized enterprise which is a business with not more than 250 employees.

"**Specification**" means the Purchaser's general requirements for the provision of services including Service Levels, set out in Schedule 1.

"Stakeholder Engagement Strategy" means a document that details the Service Provider's approach to engaging, collaborating and working effectively and with external stakeholder to enhance Service delivery and maximise Customer outcomes. The strategy must set out how the Service Provider will achieve greater integration with local services and health provision.

"Statutory Referral Organisation" or **"SRO"** means the WFS Statutory Referral Organisation (SRO) responsible for referrals. This must be made by an organisation that has been commissioned by, or has a formal contract or agreement with, an agent of a statutory body; specifically they must act on behalf of a Local Authority or NHS Board, in order to support disabled people with the highest support needs to consider and move into employment, particularly those with learning disabilities and mental health conditions.

"Supported Employment" means an internationally recognised 'place and train' model which enables disabled people to learn on the job with support from colleagues and a job coach. It is based on the principle that disabled people can obtain sustainable work in the open labour market, where they are paid the going rate for the job. In 2010, the Scottish Government published 'A Working Life for All Disabled People' - The Supported Employment Framework for Scotland which sets out our commitment to this model, which is an intensive, personalised asset-based approach.

"Sustained Job Outcome" means the outcomes as detailed in the second and third Key Performance Indicators in Annex E to Schedule 1 (Specification and Service Levels).

"Task Analysis" means looking at specific tasks within the job and developing a logical, step by step process tailored for the individual to help them carry out the task. It can also identify tasks where the individual may require extra support or training. In some cases it can identify where the task should be adapted or where support from colleagues may be necessary.

"**Tender**" means the tender submitted by the Service Provider to the Purchaser in response to the ITT dated 23rd May 2017.

"The Scottish Business Pledge" means that the Scottish Government works with local businesses and authorities to encourage them to implement the Scottish Government Business Pledge, to act on gender balance and inequality and develop city deals to generate business.

"The Scottish Government's Fair Work Agenda" means a shared vision with the Fair Work Convention that by 2025, people in Scotland will have a world-leading working life where fair work drives success, wellbeing and prosperity for individuals, businesses, organisations and society. This vision challenges not only business, employers, unions and the third sector but has clear actions for government.

"The Scottish Living Wage" means the Scottish Living Wage Accreditation Initiative that was established in April 2014 with the aim of increasing the number of employers in Scotland who are recognised for paying their staff the Living Wage. The rate for 2016/17 is £8.45.

"**TUPE**" means the Transfer of Undertakings (Protection of Employment) Regulations 2006.

"Universal Credit: Universal Credit" means a welfare benefit that supports people who are on a low income or out of work due to unemployment or heath issues. It is designed to

support households and ensure that where people are working they can sustain that employment and progress towards a life free from benefits.

"Vocational Profiling" means a person-centred tool to assist job seekers make informed choices about job preferences and establish the necessary training and support strategies for on or off the job support.

"Work Capability Assessment" means an assessment that establishes whether an ESA Customer has a limited capability for work and is, therefore, capable of engaging in work-related activity. If they do limited capability they are placed into the ESA Support Group.

"Work Related Activity" means any activity which makes it more likely that a Customer will obtain or remain in work, or be able to do so. Some Customers will be closer to the labour market than others and may be ready to enter work more quickly. Others may need to undertake some more limited activity before moving into paid work.

"**Working Day**" means a day other than a Saturday, Sunday or bank holiday in Scotland, within the meaning of the Banking and Financial Dealings Act 1971.

"**Working Hour**" means an hour between 0900 hours and 1700 hours on a Working Day.

1.2. The interpretation and construction of the Contract is subject to the following provisions:

1.2.1. words importing the singular meaning include, where the context so admits, the plural and vice versa;

1.2.2. words importing the masculine include the feminine and neuter;

1.2.3. reference to a clause is a reference to the whole of that clause unless stated otherwise;

1.2.4. references to any statute, enactment, order, regulation or other similar instrument are construed as a reference to the instrument as amended by any subsequent instrument or re-enacted;

1.2.5. references to any person include natural persons and partnerships, firms and other incorporated bodies and all other legal persons of whatever kind and however constituted and their successors and permitted assignees or transferees;

1.2.6. reference to "expiry or termination" of the Contract includes the making of a Judicial Order;

1.2.7. the words "include", "includes" and "including" are to be construed as if they were immediately followed by the words "without limitation"; and

1.2.8. headings are included in the Contract for ease of reference only and do not affect the interpretation or construction of the Contract.

2. Condition Precedent: Requirement for a Parent Company Guarantee

It shall be a condition of this Contract that, if required by the Purchaser, the Service Provider shall deliver a validly executed parent company guarantee in the form set out in Schedule 8 (Parent Company Guarantee). The rights and obligations of the Parties shall have no force or effect unless the parent company guarantee has been properly executed and delivered to the Purchaser. The parties acknowledge that if this condition has not been fulfilled any performance of this Contract by the Service Provider shall be at the risk of the Service Provider and the Purchaser shall not be liable for and the Service Provider irrevocably waives any entitlement to payment of any fees, expenses or other payments in relation to such performance. Where the Service Provider has failed to fulfil this condition within 14 days of

the Effective Date the Purchaser shall have the right to terminate the Contract by notice in writing to the Service Provider.

3. Nature of the Contract

3.1. The Contract is a public services contract within the meaning of regulation 2(1) of the Public Contracts (Scotland) Regulations 2015.

3.2. The Service Provider acknowledges that it is not the exclusive Service Provider of the Services to the Purchaser and as such no guarantee of work or volume of work has been granted or given by the Purchaser.

4. Period

4.1. Subject to the remainder of this clause 4 the period of the Contract is from and including the Effective Date to and including 2 April 2021 (unless it is terminated earlier in accordance with the provisions of the Contract), provided always that:-

4.1.1. the Service Provider shall only be entitled to receive Customer referrals pursuant to the Contract during the period commencing on the Service Commencement Date and ending on 2 April 2021 (the "**Initial Referral Period**"); and

4.1.2. the Contract shall continue for the period from (and including) 3 April 2021 in respect of those referrals made to the Service Provider prior to the expiry of the Initial Referral Period in so far as required as part of the Services which potentially could be to and including 24th November 2023.

(the "**Contract Period**").

4.2. The Purchaser may at its sole option extend the Initial Referral Period in accordance with the following provisions:

4.2.1. the Purchaser may extend the Initial Referral Period for an additional period up to (and including) 3 April 2022 by providing the Service Provider with at least sixty (60) Working Days' notice prior to the expiry of the Initial Referral Period ("**Extended Referral Period One**"); and

4.2.2. the Purchaser may extend Extended Referral Period One for an additional period up to (and including) 4 April 2023 by providing the Service Provider with at least sixty (60) Working Days' notice prior to the expiry of Extended Referral Period One ("**Extended Referral Period Two**").

4.3. Where the Initial Referral Period is extended in accordance with clause 4.2.1, clause 4.1.2 shall not apply and the Contract shall continue in respect of those referrals made to the Service Provider prior to the expiry of Extended Referral Period One in so far as required as part of the Services which potentially could be to and including 24th November 2024.

4.4. Where the Extended Referral Period One is extended in accordance with clause 4.2.2, clause 4.3 shall cease to apply and the Contract shall continue in respect of those referrals made to the Service Provider prior to the expiry of Extended Referral Period Two in so far as required as part of the Services which potentially could be to and including 24th November 2025.

4.5. Any further contractual terms required to give effect to the extensions outlined in this clause 4 shall continue in so far as necessary to take account of the relevant extension (.e.g. invoicing provisions).

5. Break

The Purchaser may terminate the Contract at any time by giving not less than three (3) months' notice to the Service Provider.

5.A Implementation

5A.1 The Service Provider shall:

5A.1.1 comply with the Implementation Plan; and

5A.1.2 ensure that each Milestone is Achieved on or before its Milestone Date.

5A.2 The Service Provider shall prepare and deliver the Detailed Implementation Plan to the Purchaser in accordance with Schedule 1 (Specification and Service Levels).

5A.3 If, at any time, the Service Provider becomes aware that it will not (or is unlikely to) successfully achieve any Milestone by the applicable Milestone Date, it shall immediately notify the Purchaser of the fact of the Delay, the reasons for the Delay, the consequences of the Delay for the rest of the Implementation Plan and how the Service Provider proposes to mitigate the Delay.

5A.4 Whether the Delay is due to the Purchaser's Default or not, the Service Provider shall deploy all additional resources and efforts, and take all reasonable steps, to eliminate or mitigate the consequences of the Delay.

5A.5 Where the Service Provider incurs additional costs as a result of any action taken or required to be taken in accordance with clause 5A.4 the Service Provider shall not be entitled to recover these from the Authority.

6. Specification and Service Levels

The Service Provider must comply with the Specification. In particular, the Service Provider must meet or exceed the Service Levels.

7. **Pricing Schedule**

7.1 The Pricing Schedule sets out details of the pricing of the Services including provision for Service Credits.

7.2. Accordingly, the Service Provider may not unilaterally increase the prices in the Pricing Schedule. For the avoidance of doubt nothing in the Contract shall prevent the Service Provider from reducing the Contract Charges.

8. Management Arrangements

8.1. The Service Provider must maintain the capacity to supply the Services throughout the Contract Period.

8.2. The Parties must comply with the Management Arrangements.

SECTION B: MISCELLANEOUS PROVISIONS INCLUDING THOSE RELATING TO PRICE, PAYMENT AND INFORMATION

9. Service Provider's Status

At all times during the Contract Period the Service Provider is an independent service provider and nothing in the Contract establishes a contract of employment, a relationship of agency or partnership or a joint venture between the Parties or between the Purchaser and any Service Provider Representative. Accordingly, neither Party is authorised to act in the name of, or on behalf of, or otherwise bind the other Party save as expressly permitted by the terms of the Contract.

10. Notices

10.1. Any notice or other communication which is to be given by a Party to the other under the Contract must be:

10.1.1. given in writing;

10.1.2. addressed in accordance with clause 10.3; and

10.1.3. sent by letter (delivered by hand, first class post or by recorded delivery or special delivery), fax or e-mail.

10.2. Provided the relevant communication is not returned or rejected as undelivered, the notice or communication is deemed to have been given:

10.2.1. 2 Working Days after the day on which the letter was posted; or

10.2.2. 4 Working Hours after the communication was sent, in the case of fax or email.

10.3. For the purposes of this clause, the address of each Party is:

10.3.1. For the Purchaser:
Scottish Government, More Powers Implementation Team, Victoria Quay, Edinburgh, EH6 6QQ
For the attention of [redacted]
Tel [redacted]
[redacted] gov.scot

10.3.2. For the Service Provider:
PeoplePlus Group Limited, Blades Enterprise Centre, John Street, Sheffield S2 4SW
For the attention of [redacted]
[redacted] peopleplus.co.uk

10.4. Either Party may change its address details by serving a notice in accordance with this clause.

10.5. Notices under clause 58.1 (Termination on Insolvency or Change of Control) may be sent to the Purchaser's trustee, receiver, liquidator or administrator, as appropriate.

11. Price

11.1. In consideration of, but subject always to, the Service Provider's performance of the Services in accordance with the Contract, the Purchaser will pay:

11.1.1. the price due in accordance with the Pricing Schedule; and

11.1.2. a sum equal to the value added tax chargeable at the prevailing rate.

11.2. The Service Provider may not suspend the provision of the Services if it considers that the Purchaser has failed to pay the price due.

12. Payment and Invoicing

12.1. The Purchaser must pay all sums due to the Service Provider within 30 days of receipt of a valid invoice.

12.2. The Service Provider must render invoices monthly in arrears.

12.3. The Service Provider must ensure that each invoice contains thje appropriate Contract references details of any Service Credits applied and a detailed breakdown of the Services provided. The Service Provider must supply such other documentation reasonably required by the Purchaser to substantiate any invoice.

12.4. Value added tax, where applicable, must be shown separately on all invoices as a strictly net extra charge.

12.5. Where any Service Credits are due to the Purchaser these shall be credited against the next invoice rendered by the Service Provider. Where no invoice is due or likely to be rendered for a period exceeding 2 months from the date the relevant Service Credit is incurred, the Service Provider must promptly issue a credit note to the Purchaser and pay the credited sum to the Purchaser within 30 days of issue.

12.6. Interest is payable on the late payment of any undisputed sums of money in accordance with the Late Payment of Commercial Debts (Interest) Act 1998. In the case of sums due by the Purchaser, the sums referred to in this clause must be properly invoiced by the Service Provider.

12.7. The Service Provider shall indemnify the Purchaser on a continuing basis against any liability, including any interest, penalties or costs incurred, that is levied, demanded or assessed on the Purchaser at any time in respect of the Service Provider's failure to account for or to pay any VAT relating to payments made to the Service Provider under this Contract. Any amounts due under this clause 12.7 shall be paid in cleared funds by the Service Provider to the Purchaser not less than five Working Days before the date upon which the tax or other liability is payable by the Purchaser.

12.8 The Service Provider shall only be entitled to claim for payments in respect of Outcomes as outlined in the Pricing Schedule for the period of three (3) months after the expiry of the Contract Period.

13. Recovery of Sums Due

13.1. Wherever under the Contract any sum of money is recoverable from or payable by the Service Provider to the Purchaser, the Purchaser may deduct that sum from any sum due to the Service Provider whether under the Contract or otherwise.

13.2. The Service Provider must make any payments due to the Purchaser without any deduction whether by way of set-off, counterclaim, discount, abatement or otherwise unless the Service Provider has a valid court order requiring an amount equal to such deduction to be paid by the Purchaser to the Service Provider.

14. Data Protection Act

14.1. For the purposes of this clause, the terms “Data Controller”, “Data Processor”, “Data Subject”, “Personal Data” and “Processing” have the meanings given in section 1(1) of the Data Protection Act 1998.

14.2. The Service Provider shall:

14.2.1. at all times comply with the Data Protection Act 1998 (including any subordinate legislation made thereunder and any guidance and/or codes of practice issued by the Information Commissioner from time to time in relation thereto) and shall not perform its obligations in such a way so as to cause the Purchaser to breach any of its obligations under the Data Protection Act 1998;

14.2.2. comply with the terms of any Data Sharing Protocol; and

14.2.3. provide all assistance, support and information required by the Purchaser in order for the Purchaser to comply with any of its obligations under the Data Protection Act 1998.

14.3. Where the Service Provider Processes Personal Data as a Data Processor for the Purchaser the Service Provider must:

14.3.1. enter into a data processing agreement in the form set out in Schedule 9 annexed hereto, and only process the Personal Data in accordance with any instructions as may be given by the Purchaser (which may be specific or of a general nature);

14.3.2. process the Personal Data only to the extent, and in such manner as is necessary for the performance of the Service Provider’s obligations under the Contract or as is required by the Law;

14.3.3. implement appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, such measures being appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;

14.3.4. obtain approval before transferring the Personal Data to any sub-contractor engaged by the Service Provider in connection with the provision of the Services (or any part of them);

14.3.5. not transfer or cause or permit the Personal Data to be transferred outside of the European Economic Area without Approval and, where the Purchaser does approve the transfer, to comply with the obligations of a Data Controller under the Eighth Data Protection Principle (as set out in Schedule 1 to the Data Protection Act 1998) and any instructions notified to the Service Provider by the Purchaser;

14.3.6. provide a written description of the technical and organisational measures employed by the Service Provider for Processing Personal Data and permit the Purchaser (on reasonable notice) to inspect and audit the Service Provider’s Processing activities;

14.3.7. ensure that all Service Provider Representatives accessing the Personal Data are competent and trained in the law of data protection and that such Service Provider

Representatives are aware of the confidential nature of the Personal Data and comply with the obligations set out in this clause;

14.3.8. not disclose or divulge (and ensure that the Service Provider Representatives do not disclose or divulge) any of the Personal Data to any third parties unless directed in writing to do so by the Purchaser;

14.3.9. allow for and contribute to audits to demonstrate compliance with this clause 14, including inspections, conducted by the Purchaser or another auditor mandated by the Purchaser;

14.3.10. inform the Purchaser immediately if, in the opinion of the Service Provider, an instruction given pursuant to clause 14.3.9 infringes any Law;

14.3.11. inform the Purchaser immediately if it becomes aware of any Personal Data breach providing such information in relation to the breach and the circumstances as the Purchaser may require and the Service Provider shall take such steps (at its cost) as the Purchaser may require in order to remedy or mitigate the breach;

14.3.12. comply with any instructions from the Purchaser in terms of the deletion or return of any Personal Data at the end of the Contract Period including those outlined in the Exit Plan; and

14.3.13. include in any sub-contracts with sub-contractor approved in accordance with clause 14.3.4 equivalent provisions as least as onerous as those set out in this clause 14.

14.3 The Service Provider must notify the Purchaser promptly, and in any event within 5 Working Days, if it receives:

14.3.1. a request from a Data Subject to have access to their Personal Data;

14.3.2 a complaint or request relating to the Purchaser's obligations under the Data Protection Act 1998;

and the Service Provider shall provide the Purchaser with full cooperation and assistance in relation to any complaint or request made.

14.4 Where the Service Provider is collecting Personal Data, the Service Provider must comply with all the fair processing provisions under the Data Protection Act 1998, and must notify the Data Subjects that the Personal Data collected by the Service Provider may be shared with the Purchaser.

14.5 The Service Provider shall indemnify the Purchaser and hold it harmless from and against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Purchaser may suffer or incur as a result of or in connection with any breach of this clause 14.

14.6 To comply with section 31(3) of the Public Services Reform (Scotland) Act 2010, the Purchaser publishes an annual statement of all payments over £25,000. In addition, in line with openness and transparency, the Scottish Government publishes a monthly report of all payments over £25,000. The Service Provider should note that where a payment is made in excess of £25,000 there will be disclosure (in the form of the name of the payee, the date of the payment, the subject matter and the amount of payment) in the both the monthly report and the annual Public Services Reform (Scotland) Act 2010 statement.

15. Freedom of Information

15.1 The Service Provider acknowledges that the Purchaser is subject to the requirements of FOISA and the Environmental Information Regulations and undertakes to assist and

cooperate with the Purchaser to enable the Purchaser to comply with FOISA and the Environmental Information Regulations.

15.2 If the Service Provider receives a Request for Information the Service Provider must promptly respond to the applicant. Where the Request for Information appears to be directed to information held by the Purchaser, the Service Provider must promptly inform the applicant in writing that the Request for Information can be directed to the Purchaser.

15.3 Where the Purchaser receives a Request for Information concerning the Contract, the Purchaser is responsible for determining at its absolute discretion whether information requested is to be disclosed to the applicant or whether the information requested is exempt from disclosure in accordance with FOISA or the Environmental Information Regulations.

15.4 The Service Provider acknowledges that the Purchaser may, acting in accordance with the Purchaser's Code of Practice on the Discharge of Functions of Public Authorities issued under section 60 of FOISA (as may be issued and revised from time to time), be obliged under FOISA or the Environmental Information Regulations to disclose information requested concerning the Service Provider or the Contract:

15.4.1 in certain circumstances without consulting the Service Provider, or

15.4.2 following consultation with the Service Provider and having taken its views into account.

15.5 Where clause 15.4 applies the Purchaser must take reasonable steps, where practicable, to give the Service Provider advance notice of the fact of disclosure or, failing that, draw the fact of disclosure to the attention of the Service Provider after such disclosure.

15.6 Where a Request for Information concerns Service Provider Sensitive Information specified in Schedule 7 (Service Provider Sensitive Information) (having regard to the justifications and durations set out there), the Purchaser must take reasonable steps, where practicable, to consult with the Service Provider before disclosing it pursuant to a Request for Information.

16 Purchaser Protected Information

16.1 The Service Provider must:

16.1.1 treat all Purchaser Protected Information as confidential and safeguard it accordingly, implementing appropriate technical and organisational measures to protect Purchaser Protected Information against disclosure;

16.1.2 only use the Purchaser Protected Information for the purposes of performing its obligations under the Contract;

16.1.3 only disclose the Purchaser Protected Information to such Service Provider Representatives that are directly involved in the performance of the Contract and need to know the information for such performance; and

16.1.4 not disclose any Purchaser Protected Information without the prior written consent of the Purchaser.

16.2 The Service Provider must immediately notify the Purchaser of any breach of security concerning the Purchaser Protected Information, providing such information in relation to the breach and the circumstances as the Purchaser may require. The Service Provider must take such steps (at its cost) as the Purchaser may require in order to remedy or mitigate the breach and fully co-operate with the Purchaser in any investigation that the Purchaser considers necessary to undertake as a result of any such breach of security.

16.3 Clause 16.1 does not apply to the extent that:

16.3.1 disclosure is required by law or by order of any competent court or tribunal;

16.3.2 information is in the possession of the Service Provider without restriction as to its disclosure prior to its disclosure by the Purchaser;

16.3.3 information is obtained from a third party (who lawfully acquired it) without restriction as to its disclosure;

16.3.4 information is already in the public domain at the time of disclosure otherwise than by a breach of the Contract; or

16.3.5 information is independently developed without access to the Purchaser Protected Information.

16.4 Breach of this clause or the Official Secrets Acts 1911 to 1989 by the Service Provider is a material breach for the purposes of clause 57.1.3 (Termination Rights).

17 Service Provider Sensitive Information

17.1 The Purchaser must:

17.1.1 treat all Service Provider Sensitive Information as confidential and safeguard it accordingly; and

17.1.2 not disclose any Service Provider Sensitive Information to any other person without the prior written consent of the Service Provider.

17.2 Clause 17.1 does not apply to the extent that:

17.2.1 disclosure is required by law or by order of any competent court or tribunal;

17.2.2 information is in the possession of the Purchaser without restriction as to its disclosure prior to its disclosure by the Service Provider;

17.2.3 information is obtained from a third party (who lawfully acquired it) without restriction as to its disclosure;

17.2.4 information is already in the public domain at the time of disclosure otherwise than by a breach of the Contract; or

17.2.5 information is independently developed without access to the Service Provider Sensitive Information.

17.3 Nothing in this Contract prevents the Purchaser from disclosing any Service Provider Sensitive Information or any other information concerning the Service Provider or the Contract:

17.3.1 pursuant to a Request for Information concerning the information (see clause 15 (Freedom of Information);

17.3.2 in accordance with the Purchaser's publication scheme (within the meaning of section 23 of FOISA) as reviewed from time to time;

17.3.3 in accordance with the requirements of Part 3 of the Public Services Reform (Scotland) Act 2010;

17.3.4 in accordance with any future policies of the Purchaser concerning the routine disclosure of government information in the interests of transparency;

17.3.5 to any consultant, Service Provider or other person engaged by the Purchaser, for example to conduct a gateway review;

17.3.6 in response to a Parliamentary Question from a Member of the Scottish Parliament, a member of the United Kingdom Parliament, or any other department, office or agency of Her Majesty's Government in Scotland or the United Kingdom, and their servants or agents, and when disclosing such information to either the Scottish Parliament or the United Kingdom Parliament it is recognised and agreed by both parties that the Purchaser shall if the Purchaser sees fit disclose such information but is unable to impose any restrictions upon the information that the Purchaser provides to Members of the Scottish Parliament or Members of the United Kingdom Parliament;

17.3.7 in response to any inquiry of the European Commission concerning the Contract; or

17.3.8 for the purpose of any examination by any auditors of the Purchaser (including Audit Scotland, the Auditor General for Scotland and the Scottish Parliament) of the economy, efficiency and effectiveness with which the Purchaser has used its resources.

17.4 The Service Provider consents to the publication of the Contract by the Purchaser, subject to such redactions as the Purchaser may decide to make. The Purchaser may consult with the Service Provider to inform its decisions concerning redaction (for example to exclude any Service Provider Sensitive Information) but any decisions taken by the Purchaser are final and conclusive.

18 Audit and Records Management

18.1 In this Clause 18, the following terms have the following meanings:-

The '**Act**' means the Public Records (Scotland) Act 2011; and

'**Records Management Plan'** means the plan prepared by the Purchaser and approved by the Keeper of the Records of Scotland under section 1 of the Act.

18.2 The Service Provider must retain and maintain until 5 years after the end of the Contract Period full and accurate records of the Contract including the Services provided and payments made and reimbursed under it.

18.3 The Service Provider must on request, and without any charge to the Purchaser, afford the Purchaser, or the Purchaser's representatives, such access to those records as may reasonably be requested by the Purchaser in connection with the Contract.

18.4 The Service Provider shall, for the duration of the Contract, provide the Purchaser with all assistance requested by the Purchaser acting reasonably to assist the Purchaser in complying with its obligations under the Act and with the Purchaser's Records Management Plan where such compliance is in respect of records created or to be created by the Service Provider on behalf of the Purchaser in terms of this Contract. This assistance will be at no cost to the Purchaser.

18.5 At the end of the Contract Period, the Service Provider shall transfer the records in question to the Purchaser, such transfer to include full ownership of the records including all Intellectual Property Rights in relation thereto. The transfer shall be at no cost to the Purchaser. The Service Provider shall ensure that all relevant information reasonably required to locate individual items within the records, including metadata and database schema, are also offered to the Purchaser on the same terms.

18.6 If the Service Provider shall become bankrupt (whether voluntarily or compulsorily), unable to pay its debts, insolvent or make arrangements with its creditors or if any resolution is adopted for the winding up of any party, or if a receiver, administrator or administrative receiver is appointed over the whole or any part of its assets or if either party goes into liquidation (whether voluntarily or compulsorily), otherwise than for the purposes of amalgamation or reconstruction or any form of execution levied upon its assets, then immediately upon the occurrence of any of these events, the records which would, in terms of clause 18.5 fall to be offered to the Purchaser shall be deemed to be held on trust by the Service Provider on behalf of the Purchaser as the Purchaser's agent. The Service Provider shall thereafter, if and when so required by the Purchaser, transfer the records in question to the Purchaser, such transfer to be on the same terms as would apply to a transfer made in terms of clause 18.5.

19 Publicity

The Service Provider must not make any press announcement or otherwise publicise the Contract in any way, except with the written consent of the Purchaser.

SECTION C: PROVISION OF SERVICES

20 Provision of the Services

20.1 The Service Provider must provide the Services:

20.1.1 in accordance with the Specification the Service Levels;

20.1.2 to the satisfaction of the Purchaser acting reasonably.

20.2 The Service Provider acknowledges that the Purchaser relies on the skill, care, diligence and judgment of the Service Provider in the supply of the Services and the performance of its obligations under the Contract.

20.3 The Service Provider must at all times implement, maintain and comply with the BCDR Plan.

21 Deliverables and Milestones

21.1 The Service Provider must provide the Services, including any Deliverables:

21.1.1 at the date(s), time(s) and location(s) required by the Purchaser; and

21.1.2 in good time to meet any Milestones required by the Purchaser.

21.2 When the Service Provider believes acting reasonably that it has provided any Deliverable or completed any Milestone in accordance with the Contract it must notify the Purchaser.

21.3 The Purchaser may thereafter by notice to the Service Provider:

21.3.1 accept the provision of the Deliverable or the completion of the Milestone (as appropriate), having regard to the Achievement criteria or any other acceptance criteria set out in the Implementation Plan or otherwise communicated to the Service Provider in writing; or

21.3.2 providing reasons, reject the provision of the Deliverable or the completion of the Milestone.

21.4 Where the Purchaser rejects the completion of a Milestone or provision of a Service or Deliverable in accordance with clause 21.3.2, the Service Provider must at its expense immediately rectify or remedy any defects and/or delays.

21.5 Risk and ownership in any Deliverables that are corporeal moveables and in any physical media in which any Deliverables are delivered vests in the Purchaser upon acceptance in accordance with this clause.

21.6 Whether the defect or delay is due to the Purchaser or not, the Service Provider shall deploy all additional resources to address the consequences of the default or delay. Where such default or delay is solely due to the Purchaser, any additional costs in respect of the said additional resources shall be agreed between the parties both acting reasonably.

21A. Assurance and Fraud Reviews

21A.1. The Service Provider must comply with the Purchaser's requirements as notified to the Service Provider by the Purchaser from time to time in respect of the three key Service Provider Assurance Areas described in clause 21A.2 below (the "**Provider Assurance Requirements**").

21A.2. The Purchaser will periodically throughout the Contract Period carry out review(s) (the "**Assurance and Fraud Review(s)**") of the Service Provider in three key Service Provider Assurance Areas:

a) **Governance Arrangements** – to ensure the Service Provider's has robust governance arrangements, systems for tracking and reporting performance and anti-fraud measures;

b) **Service Delivery** – to ensure the Service Provider's has effective systems for administering the Customer journey to ensure that the Purchaser is receiving the service it is paying for. The review will also include the management of the supply chain;

c) **Financial Procedures** – to ensure the Service Provider has effective systems in place to support their claims for payment, including appropriate segregation of duties.

21A.3. On completion of each Assurance and Fraud Review by the Purchaser, the Service provider will be awarded a Service Provider Assurance and Fraud Rating: (i) weak; or (ii) limited; or (iii) reasonable; or (iv) strong (the "**Assurance and Fraud Rating**").

21A.4. The frequency and manner of carrying out the Assurance and Fraud Reviews shall be determined at the absolute discretion of the Purchaser.

21A.5. The Purchaser shall send a formal report (the "**Assurance and Fraud Review Report**") to the Service Provider which will set out (i) the Assurance and Fraud Rating; (ii) key strengths; and (iii) weaknesses/areas for improvement.

21A.6. Without prejudice to clause 21A.9, where weakness/areas for improvement have been set out in the Assurance and Fraud Review Report, the Service Provider must submit to the Purchaser for its approval an action plan (the "**Service Provider Assurance Action Plan**") setting out appropriate steps and a proposed timetable for how the Service Provider proposes to remedy such weaknesses/areas for improvement. The Service Provider must submit the Service Provider Assurance Action Plan to the Purchaser within ten (10) Working Days (or such other period of time as notified by the Purchaser) of receipt of the Assurance and Fraud Review Report. Once the Service Provider Assurance Action Plan has been approved by the Purchaser, the Service Provider must implement it in accordance with the timetable set out in the Service Provider Assurance Action Plan.

21A.7. Where the Purchaser rejects the Service Provider Assurance Action Plan, the Service Provider shall address all of the Purchaser's concerns in a revised Service Provider Assurance Action Plan, which it shall submit to the Purchaser within a period of ten (10) Working Days (or such other period as notified by the Purchaser) of its receipt of the Purchaser's comments.

21A.8. In the event of failure to agree a timescale for the completion of the Service Provider Assurance Action Plan then the Service Provider shall have no longer than twenty eight (28) Working Days from the date of receipt to remedy the action points identified in the Service Provider Assurance and Fraud Review Report.

21A.9. Where a Service Provider Assurance Action Plan, submitted by the Service Provider is approved by the Purchaser, such approval shall not relieve the Service Provider of its obligations to remedy and weaknesses/areas for improvement set out in the Service Provider Assurance and Fraud Review Report and ensure that it does not receive a "Weak" or "Limited" Assurance and Fraud Rating in any further Service Provider Assurance and Fraud Review.

21A.10. The Purchaser accepts no liability whatsoever in respect of the content, suitability or implementation of a Service Provider Assurance Action Plan. Any assistance or advice the Purchaser may offer, or any act or omission of the Purchaser, in connection with a Service Provider Assurance Action Plan shall not relieve the Service Provider of its obligations to remedy any weaknesses/areas for improvement set out in the Service Provider Assurance and Fraud Review Report and ensure that it does not receive a "Weak" or "Limited" Assurance and Fraud Rating in any further Service Provider Assurance and Fraud Review.

21A.11. Notwithstanding that the Service Provider may have submitted and the Purchaser may have approved a Service Provider Assurance Action Plan, where a Service Provider is awarded a "Weak" or "Limited" Assurance and Fraud Rating it shall remain the Service Provider's responsibility, at its own expense, to deploy, all resources and take all action(s) necessary to remedy the "Weak" or "Limited" Assurance and Fraud Rating and ensure that it does not receive a "Weak" or "Limited" Assurance and Fraud Rating in any further Service Provider Assurance and Fraud Review.

21A.12. Failure by the Service Provider, at its own expense to deploy all resources and take all action(s) necessary to remedy the "Weak" or "Limited" Assurance and Fraud Rating shall constitute a Default by the Service Provider.

21A.13. Failure by the Service Provider:

i. to submit a Service Provider Assurance Action Plan; and/or:

ii. to submit a Service Provider Assurance Action Plan within ten (10) Working Days (or such other time period as agreed in writing by the Purchaser) of receipt of the Service Provider Assurance and Fraud Review Report; and/or

iii. to implement a Service Provider Assurance Action Plan, which has been approved by the Purchaser, in a accordance with the timetable set out in the Service Provider Assurance Action Plan;

shall constitute a Default by the Service Provider.

21A.14. The Purchaser is entitled to regard the following circumstances, without limitation, to be a material breach of the Contract which shall entitle it to terminate in accordance with clause 57.1.3 (Termination Rights).

a) Where the Service Provider has been awarded an Assurance and Fraud Rating of "Weak" or "Limited", as notified to the Service Provider by the Purchaser from time to time, in two (2) separate consecutive Service Provider Assurance and Fraud Reviews for reasons which the Purchaser regards, at its sole discretion, as similar reasons; or

b) Where the Service Provider has been awarded an Assurance and Fraud Rating of "Weak" or "Limited" as notified to the Service Provider by the Purchaser from time to time, in three (3) separate consecutive Service Provider Assurance and Fraud Reviews regardless of the reasons for such award.

21A.15. Notwithstanding any other term of the Contract, the Service Provider hereby gives its consent for the Purchaser to publish from time to time any of the Service Provider's Assurance and Fraud Ratings to the general public and to provide the Service Provider's Assurance and Fraud Ratings to any person as the Purchaser deems appropriate. The Service Provider shall assist and cooperate with the Purchaser to enable the Purchaser to publish and provide the Service Provider's Assurance and Fraud Ratings to any person the Purchaser deems appropriate in accordance with this clause.

SECTION D: STAFF INVOLVED IN THE PROVISION OF SERVICES

22 Key Individuals

22.1 The Service Provider acknowledges that the Key Individuals are essential to the proper provision of the Services to the Purchaser.

22.2 The Key Individuals must not be released from providing the Services without the approval of the Purchaser, except by reason of long-term sickness, maternity, paternity, adoption or parental leave, termination of employment or equivalent extenuating circumstances. Where such extenuating circumstances arise or are foreseeable, the Service Provider must immediately give notice of that fact to the Purchaser.

22.3 The Service Provider may propose a replacement to a Key Individual (and must do so when a Key Individual is to be released from providing the Services), in which case:

22.3.1 appropriate arrangements must be made to minimise any adverse impact on the Contract which could be caused by the change in Key Individuals (including, wherever possible, a transfer period of sufficient duration to allow for the transfer of know-how and skills); and

22.3.2 the replacement must be of at least equal status and of equivalent qualifications, experience, training and skills to the Key Individual being replaced and must be fully competent to carry out the responsibilities of that person in relation to the Services.

22.4 Any proposed replacement to a Key Individual is subject to the approval of the Purchaser. Subject to the Service Provider's compliance with this clause, the Purchaser must not unreasonably withhold such approval.

23 Offers of Employment

23.1 For the duration of the Contract and for a period of 12 months thereafter the Service Provider must not employ or offer employment to any of the Purchaser's employees who have been associated with the Contract and/or the contract management of the Contract without the Purchaser's prior approval.

23.2 This clause does not prevent the Service Provider from employing or offering employment to any person who has applied for employment in response to an advertisement placed in the normal course of business and not placed with the objective of soliciting the Purchaser's employees.

24 Staff transfer at commencement

24.1 NOT USED.

24.2 The Parties agree that the commencement of the provision of the Services by the Service Provider may constitute a Relevant Transfer in respect of the Incoming Employees.

24.3 The Service Provider is responsible for all emoluments and outgoings in respect of the Incoming Employees (including, without limitation, all wages, bonuses, commission, premiums, subscriptions, pay as you earn and national insurance contributions and pension contributions) which are attributable in whole or in part to the period from the date of the Relevant Transfer, including bonuses or commission which are payable on or before the date of the Relevant Transfer but attributable in whole or in part to the period from the date of the Relevant Transfer.

24.4 The Service Provider indemnifies the transferor against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and any other liabilities which the transferor may incur in respect of the emoluments and outgoings referred to in clause 24.3.

25 Information about Service Provider Employees

25.1 The Purchaser may by notice require the Service Provider to disclose such information as the Purchaser may require relating to those of the Service Provider's employees carrying out activities under or connected with the Contract.

25.2 The Service Provider must disclose by notice all such information as is required by the Purchaser under clause 25.1, within such reasonable period specified by the Purchaser. The Service Provider acknowledges that the Data Protection Act 1998 does not prevent the disclosure of anonymised data that is not personal data within the meaning of that Act.

25.3 The Service Provider consents to the disclosure by the Purchaser of all information provided by the Service Provider under this clause to other service providers that the Purchaser may invite to tender or appoint for services to be provided in substitution for the Services.

26 Staff transfer on expiry or termination

26.1 NOT USED.

26.2 The Parties agree that the ceasing of the provision of the Services by the Service Provider may constitute a Relevant Transfer in respect of the Outgoing Employees.

26.3 The Service Provider indemnifies the Purchaser and any replacement service provider against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Purchaser or any replacement service provider may suffer as a result of or in connection with:

26.3.1 the provision of information pursuant to clause 25;

26.3.2 any claim or demand by any Outgoing Employee (whether in contract, delict, under statute or otherwise) arising directly or indirectly from any act, fault or omission of the Service Provider in respect of any Outgoing Employee on or before the date of the Relevant Transfer;

26.3.3 any failure by the Service Provider to comply with its obligations under regulations 13 or 14 of TUPE or any award of compensation under regulation 15 of TUPE save where such failure arises from the failure of the Purchaser or any replacement service provider to comply with its obligations under regulation 13 of TUPE; and

26.3.4 any claim (including any individual employee entitlement under or consequent on such a claim) by any trade union or other body or person representing any Outgoing Employees arising from or connected with any failure by the Purchaser to comply with any legal obligation to such trade union, body or person.

26.4 The Service Provider is responsible for all emoluments and outgoings in respect of the Outgoing Employees (including, without limitation, all wages, bonuses, commission, premiums, subscriptions, pay as you earn and national insurance contributions and pension contributions) which are attributable in whole or in part to the period up to and including the date of the Relevant Transfer (including bonuses or commission which are payable after the date of the Relevant Transfer but attributable in whole or in part to the period on or before the date of the Relevant Transfer).

26.5 The Service Provider indemnifies the Purchaser and any replacement service provider against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and any other liabilities which the Purchaser or replacement service provider may incur in respect of the emoluments and outgoings referred to in clause 26.4.

27 Security

27.1 The Service Provider must comply with the Purchaser's policies concerning Baseline Personnel Security Standard clearance and such modifications to those policies or replacement policies as are notified to the Service Provider from time to time.

27.2 The Service Provider must notify the Purchaser of any matter or other change in circumstances which might adversely affect future Baseline Personnel Security Standard clearance.

27.3 The Service Provider must comply with Schedule 12 (Security) at all times when providing the Services.

SECTION E: PROVISIONS RELATING TO INTELLECTUAL PROPERTY AND GOVERNANCE

28 Parties' pre-existing Intellectual Property Rights

Except as expressly provided for in the Contract, neither Party acquires any interest in or license to use the other Party's Intellectual Property Rights as they subsist at the Effective Date or as developed independently of the Contract.

29 Specially Created Intellectual Property Rights

29.1 All Intellectual Property Rights in Deliverables and any reports, guidance, specification, instructions, toolkits, plans, data, drawings, databases, patents, patterns, models, designs or other material prepared by or for the Service Provider in the course of or in connection with

the Services for use, or intended use, in relation to the performance by the Service Provider of its obligations under the Contract belong to the Purchaser.

29.2 The Service Provider assigns to the Purchaser, with full title guarantee, all Intellectual Property Rights which may subsist in the materials referred to in clause 29.1. This assignation takes effect on the Effective Date or as an assignation of future rights that will take effect immediately on the coming into existence of the Intellectual Property Rights produced by the Service Provider. The Service Provider must execute all documentation necessary to effect this assignation.

30 Licences of Intellectual Property Rights

30.1 The Service Provider grants to the Purchaser a royalty-free, irrevocable and non-exclusive licence (with a right to sub-licence) to use any Intellectual Property Rights owned or developed prior to the Effective Date and which the Purchaser reasonably requires in order to enjoy the benefit of the Services.

30.2 Not Used

30.3 The Service Provider must ensure that the third party owner of any Intellectual Property Rights that are or which may be used to perform the Contract grants to the Purchaser a royalty-free, irrevocable and non-exclusive licence or, if itself a licensee of those rights, grants to the Purchaser an authorised and equivalently wide sub-licence, to use, reproduce, modify, develop and maintain the Intellectual Property Rights. Such licence or sub-licence must be non-exclusive, perpetual, royalty free and irrevocable.

31 Claims relating to Intellectual Property Rights

31.1 The Service Provider must not infringe any Intellectual Property Rights of any third party in providing the Services or otherwise performing its obligations under the Contract and must ensure that the provision of the Services and the use or possession of the Deliverables (or any of the materials referred to at clause 29.1) does not infringe such Intellectual Property Rights.

31.2 The Service Provider must promptly notify the Purchaser if any claim or demand is made or action brought against the Service Provider for infringement or alleged infringement of any Intellectual Property Right which may affect the use or possession of the Deliverables (or any of the materials referred to at clause 29.1) or which may affect the provision of the Services.

31.3 Where a claim to which this clause applies is made, the Service Provider must, at its expense, use its best endeavours to:

31.3.1 modify the relevant Services or Deliverables or materials (as the case may be)or substitute alternative Services or Deliverables or materials (in any case without reducing performance or functionality) so as to avoid the infringement or alleged infringement of the Intellectual Property Rights; or

31.3.2 procure the grant of a licence or licences from the pursuer, claimant or complainer, on terms acceptable to the Purchaser, so as to avoid the infringement or alleged infringement of the Intellectual Property Rights of the pursuer, claimant or complainer.

31.4 The Service Provider must not without the consent of the Purchaser make any admissions which may be prejudicial to the defence or settlement of any claim to which this clause applies.

31.5 The Service Provider shall indemnify the Purchaser and hold it harmless from and against all actions, suits, claims, demands, losses, charges, damages, costs and expenses and other liabilities which the Purchaser may suffer or incur as a result of or in connection with any breach of this clause 31.

32 Assignation

32.1 The Service Provider may not assign its interest in the Contract or any part of it without the prior written consent of the Purchaser.

32.2 Notwithstanding clause 32.1, the Service Provider may assign to another person (an "**Assignee**") the right to receive the price due to the Service Provider under the Contract subject to:

32.2.1 deduction of sums in respect of which the Purchaser exercises its right of recovery under clause 13 (Recovery of Sums Due); and

32.2.2 all the related rights of the Purchaser under the Contract in relation to the recovery of sums due but unpaid.

32.3 The Service Provider must notify or ensure that any Assignee notifies the Purchaser of any variations to the arrangements for making payments or for handling invoices, in each case in good time to enable the Purchaser to redirect payments or invoices accordingly. In the absence of such notification the Purchaser is under no obligation to vary its arrangements for making payments or for handling invoices.

32.4 Subject to clause 32.6, the Purchaser may assign, novate or otherwise dispose of its rights and obligations under the Contract or any part thereof to:

(a) any Contracting Authority; or

(b) any other body established by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Purchaser; or

(c) any private sector body which substantially performs the functions of the Purchaser,

provided that any such assignation, novation or other disposal shall not increase the burden of the Service Provider's obligations under the Contract.

32.5 Any change in the legal status of the Purchaser such that it ceases to be a Contracting Authority shall not, subject to clause 32.6, affect the validity of the Contract. In such circumstances, the Contract shall bind and inure to the benefit of any successor body to the Purchaser.

32.6 If the rights and obligations under the Contract are assigned, novated or otherwise disposed of pursuant to clause 32.4 to a body which is not a Contracting Authority or if there is a change in the legal status of the Purchaser such that it ceases to be a Contracting Authority (in the remainder of this clause both such bodies being referred to as the **"Transferee"**):

(a) the rights of termination of the Purchaser in clauses 57 (Termination Rights) and 58 (Termination on Insolvency and Change of Control) shall be available to the Service Provider in the event of respectively, the bankruptcy or insolvency, or Default of the Transferee; and

(b) the Transferee shall only be able to assign, novate or otherwise dispose of its rights and obligations under the Contract or any part thereof with the prior consent in writing of the Service Provider.

32.7 The Purchaser may disclose to any Transferee any confidential information of the Service Provider (including the Service Provider Sensitive Information) which relates to the performance of the Service Provider's obligations under the Contract. In such circumstances the Purchaser shall authorise the Transferee to use such confidential information only for purposes relating to the performance of the Service Provider's obligations under the Contract and for no other purpose and shall take all reasonable steps to ensure that the Transferee gives a confidentiality undertaking in relation to such confidential information.

33 Change of Control

The Service Provider must notify the Purchaser:

33.1 whenever it proposes to undergo a change of Control, or a change of control is likely to occur; and

33.2 immediately following a change of Control that has occurred.

34 Sub-Contracting

34.1 The Purchaser approves the appointment of the sub-contractors specified in Schedule 6 (Approved Sub-contractors) in respect of the obligations specified in that Schedule.

35 The Service Provider may not sub-contract its obligations under the Contract to other sub contractors without the prior written consent of the Purchaser. Sub-contracting of any part of the Contract shall not relieve the Service Provider of any obligation or duty attributable to the Service Provider under the Contract. The Service Provider shall be responsible for the acts and omissions of its sub-contractors as though they are its own.

35.1 Where the Service Provider enters into a sub-contract the Service Provider must ensure that a provision is included which:

35.1.1 requires payment to be made of all sums due by the Service Provider to the sub-contractor within a specified period not exceeding 30 days from the receipt of a valid invoice as defined by the sub-contract requirements and provides that, where the Purchaser has made payment to the Service Provider in respect of Services and the sub-contractor's invoice relates to such Services then, to that extent, the invoice must be treated as valid and, provided the Service Provider is not exercising a right of retention or set-off in respect of a breach of contract by the sub-contractor or in respect of a sum otherwise due by the sub-contractor to the Service Provider, payment must be made to the sub-contractor without deduction;

35.1.2 notifies the sub-contractor that the sub-contract forms part of a larger contract for the benefit of the Purchaser and that should the sub-contractor have any difficulty in securing the timely payment of an invoice, that matter may be referred by the sub-contractor to the Purchaser;

35.1.3 requires that all contracts with subcontractors and suppliers which the subcontractor intends to procure, and which the subcontractor has not before the date of this Contract, already planned to award to a particular supplier are advertised through the Public Contracts Scotland procurement portal (www.publiccontractsscotland.gov.uk) and awarded following a fair, open, transparent and competitive process proportionate to the nature and value of the contract; and

35.1.4 is in the same terms as that set out in this clause 34.3 (including for the avoidance of doubt this clause 34.3.4) subject only to modification to refer to the correct

designation of the equivalent party as the Service Provider and sub-contractor as the case may be.

35.2 The Service Provider shall also include in every sub-contract:

35.2.1 a right for the Service Provider to terminate that sub-contract if the relevant sub-contractor fails to comply in the performance of its contract with legal obligations in the fields of environmental, social or employment law or if any of the termination events (involving substantial modification of the Contract, contract award despite the existence of exclusion grounds or a serious infringement of EU legal obligations) specified in clause 57.3 occur; and

35.2.2 a requirement that the sub-contractor includes a provision having the same effect as 34.4.1 in any sub-contract which it awards.

In this clause 34.4, '**sub-contract**' means a contract between two or more service providers, at any stage of remoteness from the Purchaser in a sub-contracting chain, made wholly or substantially for the purpose of performing (or contributing to the performance of) the whole or any part of this Contract.

35.3 Where requested by the Purchaser, copies of any sub-contract must be sent by the Service Provider to the Purchaser as soon as reasonably practicable.

35.4 Where the Service Provider proposes to enter into a sub-contract it must:

35.4.1 advertise its intention to do so in at least one trade journal, at least one newspaper circulating in Scotland and the Public Contracts Scotland Portal; and

35.4.2 follow a procedure leading to the selection of the sub-contractor which ensures reasonable competition following principles of equal treatment, non-discrimination and transparency and which ensures that such procedure is accessible by small and medium enterprises.

36 Change

Change Control Procedure

35.1 Any requirement for a Change shall be subject to the Change Control Procedure.

Change in Law

35.2 The Service Provider shall neither be relieved of its obligations to supply the Services in accordance with the terms and conditions of the Contract nor be entitled to an increase in the Contract Charges as the result of a Change in Law.

SECTION F SERVICE PROVIDER CONDUCT REQUIREMENTS

36 Compliance with the Law etc.

In providing the Services and otherwise when performing the Contract, the Service Provider must comply in all respects with:

36.1 all applicable Law;

36.2 any applicable requirements of regulatory bodies; and

36.3 Good Industry Practice.

37 Official Secrets Acts

The Service Provider undertakes to abide and procure that the Service Provider's employees abide by the provisions of the Official Secrets Acts 1911 to 1989.

38 Service Provider's responsibility for staff etc.

38.1 The Service Provider is responsible for the acts and omissions of all Service Provider Representatives relating to the Contract as though such acts and omissions are the Service Provider's own.

38.2 The Service Provider must ensure that all Service Provider Representatives:

38.2.1 are appropriately experienced, skilled, qualified and trained;

38.2.2 carry out their activities connected with the Contract faithfully and diligently and with all with due skill, care and diligence; and

38.2.3 obey all lawful and reasonable directions of the Purchaser when carrying out activities under the Contract.

39 Access to the Purchaser's premises

39.1 Any access to, or occupation of, the Purchaser's premises which the Purchaser may (at its discretion) grant the Service Provider from time to time is on a non-exclusive licence basis free of charge. The Service Provider must use the Purchaser's premises solely for the purpose of performing its obligations under the Contract and must limit access to the Purchaser's premises to such individuals as are necessary for that purpose.

39.2 The Service Provider must comply with the Purchaser's policies concerning Baseline Personnel Security Standard clearance and such modifications to those policies or replacement policies as are notified to the Service Provider from time to time.

39.3 At the Purchaser's written request, the Service Provider must provide a list of the names and addresses of all persons who may require admission to the Purchaser's premises in connection with the Contract, specifying the capacities in which they are concerned with the Contract and giving such other particulars as the Purchaser may reasonably request.

39.4 The Service Provider must ensure that any individual Service Provider Representative entering the Purchaser's premises has completed the process for obtaining Baseline Personnel Security Standard clearance. The Service Provider acknowledges that the Purchaser has the right to deny entry to any individual that has not completed the process for obtaining Baseline Personnel Security Standard clearance.

39.5 In accordance with the Purchaser's policies concerning visitor access, entry to the Purchaser's premises may be granted to individual Service Provider Representatives for the purposes of meetings, notwithstanding that the process for obtaining Baseline Personnel Security Standard clearance has not commenced or completed.

39.6 The Purchaser may, by notice to the Service Provider, refuse to admit onto, or withdraw permission to remain on, the Purchaser's premises any Service Provider Representative whose admission or continued presence would, in the opinion of the Purchaser acting reasonably, be undesirable.

39.7 The Purchaser must provide advice and assistance acting reasonably to the Service Provider to facilitate the Service Provider's compliance with this clause.

39.8 All decisions of the Purchaser under this clause are final and conclusive.

40 Service Provider's Equipment

40.1 The Service Provider must provide all Equipment necessary to perform any required activities on the Purchaser's premises or otherwise necessary for the provision of Services.

40.2 But the Service Provider must not, without the Purchaser's approval:

40.2.1 bring Equipment onto the Purchaser's premises; or

40.2.2 leave Equipment on the Purchaser's premises.

40.3 Any Equipment brought onto the Purchaser's premises:

40.3.1 remains the property of the Service Provider; and

40.3.2 is at the Service Provider's own risk and the Purchaser has no liability for any loss of or damage to the Equipment unless the Service Provider is able to demonstrate that such loss or damage was caused or contributed to by the Purchaser's Default.

40.4 The Service Provider must keep all Equipment brought onto the Purchaser's premises in a safe, serviceable and clean condition. The Purchaser may at any time require the Service Provider to remove from the Purchaser's premises any Equipment which in the opinion of the Purchaser acting reasonably is either hazardous, noxious or not in accordance with the Contract and substitute proper and suitable Equipment at the Service Provider's expense as soon as reasonably practicable.

40.5 On completion of any required activities on the Purchaser's premises or at the end of a Working Day (as appropriate), the Service Provider must at its own expense:

40.5.1 remove all Equipment; and

40.5.2 leave the premises in a clean, safe and tidy condition, clearing away all rubbish arising out of the Service Provider's activities.

40.6 The Service Provider is solely responsible for making good any damage to the Purchaser's premises or any objects contained therein, other than wear and tear, which is caused by the Service Provider.

41 Purchaser Property

41.1 Where the Purchaser issues Purchaser Property to the Service Provider, the Purchaser Property remains at all times the property of the Purchaser.

41.2 The Service Provider undertakes the safe custody of the Purchaser Property and to that end must:

41.2.1 keep the Purchaser Property in good order and condition (excluding wear and tear);

41.2.2 comply with any particular security requirements communicated to the Purchaser in relation to the Purchaser Property;

41.2.3 use any Purchaser Property solely in connection with the Contract and for no other purpose; and

41.2.4 store the Purchaser Property separately and ensure that it is clearly identifiable as belonging to the Purchaser.

41.3 The Purchaser Property is deemed for the purposes of clause 41.2.1 to be in good order and condition when received by the Service Provider unless the Service Provider notifies the Purchaser otherwise within 5 Working Days of receipt.

41.4 The Service Provider must not:

41.4.1 modify or replace the Purchaser Property;

41.4.2 use the Purchaser Property as security for a loan or other obligation;

41.4.3 sell, or attempt to sell or part with possession of the Purchaser Property; or

41.4.4 allow anyone to obtain a lien over, or right to retain, the Purchaser Property.

41.5 The Service Provider licences the Purchaser to enter any premises of the Service Provider during Working Hours on reasonable notice to recover any Purchaser Property.

41.6 The Service Provider undertakes the due return of the Purchaser Property and as such is liable for all loss of, or damage to, the Purchaser Property (excluding wear and tear), unless such loss or damage was caused or contributed to by the Purchaser's Default. The Service Provider must notify the Purchaser promptly and, in any event within 2 Working Days, upon becoming aware of any defects appearing in or losses or damage occurring to the Purchaser Property.

42 Health and Safety etc.

42.1 While on the Purchaser's premises, the Service Provider must comply with the Purchaser's policies concerning health and safety and fire and such modifications to those policies or replacement policies as are notified to the Service Provider from time to time.

42.2 The Service Provider must immediately inform the Purchaser in the event of any incident occurring in the performance of its obligations under the Contract on the Purchaser's premises where that incident causes any personal injury or damage to property which could give rise to personal injury. The Service Provider must then promptly notify the Purchaser of that fact.

42.3 The Purchaser must promptly notify the Service Provider of any health and safety hazards which may exist or arise at the Purchaser's premises and which may affect the Service Provider in the performance of its obligations under the Contract.

42.4 The Service Provider must promptly make available its statutory health and safety policy statement to the Purchaser on request.

42.5 The Service Provider shall promptly notify the Purchaser of any health and safety hazards which may arise in connection with the performance of the Services (including any which occur on the premises of Service Provider Representatives).

42.6 The Service Provider shall notify the Purchaser immediately in the event of any incident occurring in the performance of the Services (including any incident which occurs on the premises of Service Provider Representatives) where that incident has caused any personal injury or damage to property or which could have caused personal injury or damage to property.

42.7 The Service Provider shall comply (and ensure that all Service Provider Representatives comply) with the requirements of the Health and Safety at Work Act etc.1974 and any other applicable Law relating to health and safety, which may apply in the performance of the Services.

42.8 The Service Provider shall ensure that its health and safety policy statement (as required by the Health and Safety at Work Act etc.1974) is made available to the Purchaser on request.

42A. Effective Procedures

42A.1 The Service Provider shall have sufficiently robust procedures in place at all times to minimise the risk that Service Provider Representatives could pose to Customers.

42A.2 The Service Provider shall ensure that in respect of any Service Provider Representatives who will come into direct contact with any Customers that the Service Provider (or relevant third party employer) has received, reviewed and is content with the terms of a basic disclosure certificate from Disclosure Scotland in respect of the relevant individual (with updated satisfactory certificates to be received and reviewed periodically throughout the employment of the relevant individual). If at any time, the provision of the Services requires enhanced Disclosure Scotland security clearances / certificates the Service Provider shall be responsible for ensuring compliance with any such enhanced requirements.

42A.3 It shall be at the Service Provider's sole responsibility and cost to ensure that the necessary Disclosure Scotland security clearances / certificates are being complied with. The Purchaser shall have a right to audit the Service Provider's compliance with this clause at any time during the Contract Period.

43 Offences

43.1 The Service Provider must not commit or attempt to commit any offence:

43.1.1 under the Bribery Act 2010;

43.1.2 of fraud, uttering, or embezzlement at common law; or

43.1.3 of any other kind referred to in regulation 58(1) of the Public Contracts (Scotland) Regulations 2015.

43.2 In performing its obligations under this Contract, the Service Provider shall, and shall ensure that each of its sub-contractors shall, comply with the terms of the Modern Slavery Act 2015 and all applicable regulations and codes in force in relation thereto.

43.3 Breach of clause 43 is a material breach for the purposes of clause 57.1.3 (Termination Rights).

44 Tax Arrangements

44.1 Where the Service Provider is liable to be taxed in the UK in respect of consideration received under this contract, it shall at all times comply with the Income Tax (Earnings and Pensions) Act 2003 (ITEPA) and all other statutes and regulations relating to income tax in respect of that consideration.

44.2 Where the Service Provider is liable to National Insurance Contributions (NICs) in respect of consideration received under this contract, it shall at all times comply with the Social Security Contributions and Benefits Act 1992 (SSCBA) and all other statutes and regulations relating to NICs in respect of that consideration.

44.3 The Purchaser may, at any time during the Contract Period, request the Service Provider to provide information which demonstrates how the Service Provider complies with sub-clauses 44.1 and 44.2 above or why those clauses do not apply to it.

44.4 A request under sub-clause 44.3 above may specify the information which the Service Provider must provide and the period within which that information must be provided.

44.5 The Purchaser may supply any information which it receives under clause 44 to the Commissioners of Her Majesty's Revenue and Customs for the purpose of the collection and management of revenue for which they are responsible.

44.6 The Service Provider shall take all reasonable steps to ensure the observance of the provisions of this clause 44 by all of their servants, employees, agents, consultants and sub-contractors.

44.7 Where the Service Provider enters into any sub-contract with any of its servants, employees, agents, consultants and/or sub-contractors, the Service Provider must ensure that a provision is included which is in the same terms as this clause 44 subject only to modification to refer to the correct designation of the equivalent party as the Service Provider.

44.8 The Service Provider shall indemnify the Purchaser against any income tax, national insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made in connection with the provision of the Services by the Service Provider or any Service Provider Representatives.

45 Discrimination

The Service Provider must not unlawfully discriminate against any person within the meaning of the Equality Act 2010 in its activities relating to the Contract or any other contract with the Purchaser.

46 Blacklisting

The Service Provider must not commit any breach of the Employment Relations Act 1999 (Blacklists) Regulations 2010 or section 137 of the Trade Union and Labour Relations (Consolidation) Act 1992, or commit any breach of the Data Protection Act 1998 by unlawfully processing personal data in connection with any blacklisting activities. Breach of this clause is a material breach of the Contract which shall entitle the Purchaser to terminate in accordance with clause 57.1.3 (Termination Rights).

47 Sustainability etc.

47.1 The Service Provider must ensure that the Services are performed in accordance with the Scottish Government's environmental policy, which is to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone-depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment.

47.2 The Service Provider shall meet all requirements of the Scottish Government's sustainability policies, details of which can be found using website referred to below and which the Service Provider shall be deemed to be aware of:

http://www.scotland.gov.uk/Topics/Environment/SustainableDevelopment

48 Conflicts of interest

48.1 The Service Provider must take appropriate steps to ensure that the Purchaser is not placed in a position where, in the reasonable opinion of the Purchaser, there is an actual or potential conflict between the interests of the Service Provider and the duties owed to the Purchaser under the Contract.

48.2 The Service Provider must disclose by notice to the Purchaser full particulars of any actual or potential conflict of interest which may arise and must take such steps as are necessary to avoid or remove the conflict of interest.

48.3 Breach of this clause by the Service Provider is a material breach for the purposes of clause 57.1.3 (Termination Rights).

SECTION G FINAL PROVISIONS

49 Warranties and Representations

The Service Provider warrants and represents that:

49.1 it has full capacity and authority and all necessary consents (including where its procedures so require, the consent of its parent company) to enter into and perform its obligations under the Contract and that the Contract is executed by a duly authorised individual;

49.2 in entering the Contract it has not committed any offence under the Bribery Act 2010 or of fraud or uttering at common law or any other kind referred to in the Public Contracts (Scotland) Regulations 2015;

49.3 it has not committed any breach of the Employment Relations 1999 Act (Blacklists) Regulations 2010 or section 137 of the Trade Union and Labour Relations (Consolidation) Act 1992, or committed any breach of the Data Protection Act 1998 by unlawfully processing personal data in connection with any blacklisting activities;

49.4 as at the Effective Date, all information contained in the ESPD and Tender remains true, accurate and not misleading, save as may have been specifically disclosed in writing to the Purchaser prior to execution of the Contract;

49.5 no claim is being asserted and no litigation, alternative dispute resolution procedure or administrative proceeding is presently in progress or, to the best of its knowledge and belief, pending or threatened against it or any of its assets which will or might have a material adverse effect on its ability to perform its obligations under the Contract;

49.6 it is not subject to any contractual obligation, compliance with which is likely to have a material adverse effect on its ability to perform its obligations under the Contract;

49.7 no proceedings or other steps have been taken and not discharged (nor, to the best of its knowledge, are threatened) for the winding up of the Service Provider or for its dissolution or for the appointment of a receiver, administrative receiver, liquidator, manager, administrator or similar officer in relation to any of the Service Provider's assets or revenue;

49.8 it owns, has obtained or is able to obtain, valid licences for all Intellectual Property Rights that are necessary for the performance of its obligations under the Contract;

49.9 in the 3 years prior to the Effective Date:

49.9.1 it has conducted all financial accounting and reporting activities in compliance in all material respects with the generally accepted accounting principles that apply to it in any country where it files accounts;

49.9.2 it has been in full compliance with all applicable securities and tax laws and regulations in the jurisdiction in which it is established;

49.10 it has not done or omitted to do anything which could have a material adverse effect on its assets, financial condition or position as an ongoing business concern or its ability to fulfil its obligations under the Contract;

49.11 it has made appropriate inquiries (for example as regards the Purchaser's premises) so as to be satisfied in relation to all matters connected with the performance of its obligations under the Contract;

49.12 it is familiar with the Purchaser's policies concerning Baseline Personnel Security Standard clearance and health and safety and fire as they apply at the Effective Date;

49.13 it has in place appropriate technical and organisational measures to safeguard any Purchaser Protected Information provided by the Purchaser;

49.14 there are no actual or potential conflicts between the interests of the Service Provider and the duties owed to the Purchaser under the Contract, save as may have been specifically disclosed in writing to the Purchaser prior to execution of the Contract; and

49.15 it is deemed to have inspected any premises at which the services are to be performed as set out in the Specification (the 'Premises') before tendering so as to have understood the nature and extent of the Services to be carried out and is deemed to be satisfied in relation to all matters connected with the Services and the Premises.

50 General Indemnity

The Service Provider shall indemnify the Purchaser against all claims, proceedings, actions, damages, costs, charges, expenses and any other liabilities which may arise out of, or in consequence of, any Default of the Service Provider.

51 Limitation of Liability

51.1 Subject to clause 51.2, neither Party is liable to the other Party under the Contract for any:

51.1.1 loss of profits, business, revenue or goodwill; or

51.1.2 indirect or consequential loss or damage.

51.2 Clause 51.1 shall not exclude any liability of the Service Provider for additional operational, administrative costs or expenses or wasted expenditure resulting from the direct Default of the Service Provider.

51.3 Subject to clauses 51.5 and 51.6, the aggregate liability of the Service Provider to the Purchaser for any one incident or a series of related incidents occurring in any Contract Year for Defaults under or in connection with the Contract shall in no event exceed 200% of the Contract Charges paid or payable in the relevant Contract Year in which the liability arises (on the basis that the Services had been properly performed) .

51.4 Subject to clause 51.6, the aggregate liability of the Purchaser to the Service Provider in any Contract Year for Defaults under or in connection with the Contract shall in no event exceed 100% of the Contract Charges paid or payable in the relevant Contract Year in which the liability arises.

51.5 The Service Provider's liability to the Purchaser under any of the following clauses shall be unlimited:-

51.5.1 clause 12.7 (Payment and Invoicing);

51.5.2 clause 14 (Data Protection Act);

51.5.3 clause 16 (Purchaser Protected Information);

51.5.4 clause 24 (Staff Transfer at Commencement);

51.5.5 clause 26 (Staff Transfer on Expiry or Termination);

51.5.6 clause 27 (Security)

51.5.7 clause 31 (Claims relating to Intellectual Property Rights);

51.5.8 clause 43 (Offences);

51.5.9 clause 44.8 (Tax Arrangements);

51.5.10 clause 45 (Discrimination);

51.5.11 clause 46 (Blacklisting); and

51.5.12 clause 49.1 and 49.2 (Warranties and Representations).

51.6 Neither Party excludes or limits liability to the other Party for:

51.6.1. death or personal injury caused by its negligence;

51.6.2. misrepresentation;

51.6.3. any breach of any obligations implied by section 12 of the Sale of Goods Act 1979 or sections 2 or 11B of the Supply of Goods and Services Act 1982; or

51.6.4 any liability to the extent that it cannot be limited or excluded by Law.

52 Insurances

52.1 The Service Provider must effect and maintain with a reputable insurance company:

52.1.1 public liability insurance in the sum of not less than **twenty million pounds** (**£ 20,000,000)**;

52.1.2 professional indemnity insurance in the sum of not less than **ten million pounds** (**£ 10,000,000)** and

52.1.3 employer's liability insurance in accordance with any legal obligation for the time being in force.

52.2 Such insurance must be maintained for the Contract Period and for a minimum of 5 years following the expiry or termination of the Contract.

52.3 The Service Provider must give the Purchaser, on request, copies of all insurance policies referred to in this clause or a broker's verification of insurance to demonstrate that the appropriate cover is in place, together with receipts or other evidence of payment of the latest premiums due under those policies.

53 Force Majeure

53.1 Neither Party is liable to the other Party for any delay in performing, or other failure to perform, its obligations under the Contract to the extent that such delay or failure is a result of Force Majeure. Nonetheless, each Party must use all reasonable endeavours to continue to perform its obligations under the Contract for the duration of such Force Majeure. However, if Force Majeure prevents either Party from performing its material obligations under the Contract for a period in excess of 90 Days, either Party may terminate the Contract with immediate effect by notice.

53.2 Any delay or other failure by the Service Provider in performing its obligations under the Contract which results from any failure or delay by a Service Provider Representative is only to be regarded as due to Force Majeure if that Service Provider Representative is itself impeded by Force Majeure from complying with an obligation to the Service Provider.

53.3 If either Party becomes aware of Force Majeure which gives rise to, or is likely to give rise to, any delay or failure on its part as described in clause 53.1, it must immediately notify the other Party of the Force Majeure and the estimated period for which the failure or delay is to continue.

53.4 The only events that afford relief from liability for failure or delay under the Contract are Force Majeure events.

54 Dispute Resolution

54.1 The Parties must attempt in good faith to resolve any dispute between them arising out of or in connection with the Contract in accordance with the Management Arrangements.

54.2 Subject to clause 59.2, any dispute or difference arising out of or in connection with the Contract, including any question regarding its existence, validity or termination, which cannot be resolved in accordance with the Management Arrangements, shall be determined by the appointment of a single arbitrator to be agreed between the Parties, and failing agreement within 14 days after either Party has given to the other a written request to concur in the appointment of an arbitrator, by an arbitrator to be appointed by the Scottish Arbitration Centre on the written application of either Party. The seat of the arbitration shall be in Scotland. The language used in the arbitral proceedings shall be English.

54.3 Any arbitration under clause 54.2 is subject to the Arbitration (Scotland) Act 2010.

55 Severability

If any provision of the Contract is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision is severed and the remainder of the provisions of the Contract continue in full force and effect as if the Contract had been executed with the invalid, illegal or unenforceable provision eliminated.

56 Waiver and Cumulative Remedies

56.1 Any failure of either Party to insist upon strict performance of any provision of the Contract, or the failure of either Party to exercise, or any delay in exercising, any right or remedy does not constitute a waiver of that right or remedy and does not cause a diminution of the obligations established by the Contract.

56.2 Accordingly, no waiver is effective unless it is expressly stated to be a waiver and communicated to the other Party in writing in accordance with clause 10 (notices).

56.3 A waiver of any Default is not a waiver of any subsequent Default.

56.4 The rights and remedies provided by the Contract are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy is not to be deemed an election of such remedy to the exclusion of other remedies.

57 Termination Rights

57.1 The Purchaser may terminate the Contract by notice to the Service Provider with immediate effect if the Service Provider commits a Default and:

57.1.1 the Service Provider has not remedied the Default to the satisfaction of the Purchaser within 20 Working Days, or such other period as may be specified by the Purchaser, after issue of a notice specifying the Default and requesting it to be remedied;

57.1.2 the Default is not in the opinion of the Purchaser, capable of remedy; or

57.1.3 the Default is a material breach of the Contract; or

57.1.4 without prejudice to clause 57.1.1 to 57.1.3, the Default concerns the Service Provider's repeated or persistent failure to meet the Service Levels (or any of them).

57.2 The Purchaser may also terminate the Contract in accordance with any provisions of the Schedules which permit the Purchaser to do so.

57.3 The Purchaser may terminate the Contract in the event that:

(a) the Contract has been subject to substantial modification which would have required a new procurement procedure in accordance with regulation 72(9) (modification of contracts during their term) of The Public Contracts (Scotland) Regulations 2015;

(b) the Service Provider has, at the time of contract award, been in one of the situations referred to in regulation 58(1) (exclusion grounds) of The Public Contracts (Scotland) Regulations 2015, including as a result of the application of regulation 58(2) of those regulations, and should therefore have been excluded from the procurement procedure; or

(c) the Contract should not have been awarded to the Service Provider in view of a serious infringement of the obligations under the Treaties and the Directive

2014/24/EU that has been declared by the Court of Justice of the European Union in a procedure under Article 258 of the Treaty on the Functioning of the European Union.

In this Condition, 'the Treaties' has the meaning given in the European Communities Act 1972.

57.4 The Purchaser may also terminate the Contract in the event of a failure by the Service Provider to comply in the performance of the Services with legal obligations in the fields of environmental, social or employment law.

58 Termination on Insolvency and Change of Control

58.1 The Service Provider shall notify in writing immediately, and the Purchaser may terminate the Contract with immediate effect by notice, where in respect of the Service Provider:

58.1.1 a proposal is made for a voluntary arrangement within Part I of the Insolvency Act 1986 or of any other composition scheme or arrangement with, or assignation for the benefit of, its creditors;

58.1.2 a shareholders' meeting is convened for the purpose of considering a resolution that it be wound up or a resolution for its winding-up is passed (other than as part of, and exclusively for the purpose of, a bona fide reconstruction or amalgamation);

58.1.3 a petition is presented for its winding up (which is not dismissed within 14 days of its service) or an application is made for the appointment of a provisional liquidator or a creditors' meeting is convened pursuant to section 98 of the Insolvency Act 1986;

58.1.4 a receiver, administrative receiver or similar officer is appointed over the whole or any part of its business or assets;

58.1.5 an application order is made either for the appointment of an administrator or for an administration order, an administrator is appointed, or notice of intention to appoint an administrator is given;

58.1.6 it is or becomes insolvent within the meaning of section 123 of the Insolvency Act 1986;

58.1.7 being a "small company" within the meaning of section 382 of the Companies Act 2006, a moratorium comes into force pursuant to schedule A1 to the Insolvency Act 1986;

58.1.8 a debt relief order is entered into; or

58.1.9 any event similar to those listed above occurs under the law of any other jurisdiction.

58.2 The Purchaser may terminate the Contract by notice with immediate effect within 6 months of:

58.2.1 being notified that a change of Control has occurred in accordance with clause 33.2 (Change of Control); or

58.2.2 where no such notification has been given, the date that the Purchaser becomes aware of the change of control.

58.3 But the Purchaser may not terminate the Contract under clause 58.2 where approval of the change of control has been granted by notice by the Purchaser.

59 Exit Management

59.1 The Service Provider shall comply with the provisions of Schedule Part 10 (Exit Management) and any current Exit Plan in relation to orderly transition of the Services to the Purchaser or the Replacement Service Provider.

59.2 The Service Provider agrees that if it breaches (or attempts or threatens to breach) its obligation to provide Exit Management, the Purchaser and their respective customers and stakeholders shall be irreparably harmed. In such circumstance, the Service Provider agrees that the Purchaser may proceed directly to court in accordance with clause 61 (Governing Law and Jurisdiction) notwithstanding anything to the contrary in the dispute resolution procedure outlined in Clause 54 (Dispute Resolution). If a court of competent jurisdiction finds that the Service Provider has breached (or attempted or threatened to breach) any such obligation, the Service Provider agrees that without any additional findings of irreparable injury, or other conditions to interdict, the Service Provider shall not oppose the entry of an appropriate order compelling performance by the Service Provider and restraining the Service Provider from any further breaches or attempted or threatened breaches of its obligations in relation to Exit Management.

60 Consequences of Expiry or Termination

60.1 Where the Purchaser terminates the Contract under clause 57 (Termination Rights) and makes other arrangements for the provision of services, the Service Provider indemnifies the Purchaser against all costs incurred in making those arrangements.

60.2 Where the Purchaser terminates the Contract under clause 5 (Break), the Purchaser indemnifies the Service Provider against any unavoidable losses directly resulting from the termination of the Contract.

60.3 The indemnity given by the Purchaser under clause 60,2 is subject to the Service Provider:

60.3.1 taking all reasonable steps to mitigate its loss;

60.3.2 taking all reasonable steps to recover its losses under any insurance policies held by it; and

60.3.3 submitting a fully itemised and costed list of losses which it seeks to recover from the Purchaser together with supporting evidence.

60.4 On expiry or termination of the Contract the Service Provider must:

60.4.1 immediately return to the Purchaser all Purchaser Property and Purchaser Protected Information in its possession; and

60.4.2 destroy or delete any copies of Purchaser Protected Information (whether physical or electronic) in its possession.

60.5 The following provisions survive the expiry or termination of the Contract:

60.5.1 clause 1 (Definitions and Interpretation);

60.5.2 clause 13 (Recovery of Sums Due);
60.5.3 clause 14 (Data Protection Act);
60.5.4 clause 15 (Freedom of Information);
60.5.5 clause 16 (Purchaser Protected Information);
60.5.6 clause 17 (Service Provider Sensitive Information);
60.5.7 clause 18 (Audit and Records Management);
60.5.8 clause 19 (Publicity);
60.5.9 clause 23 (Offers of Employment);
60.5.10 clause 25 (Information about Service Provider Employees);

60.5.11 clause 26 (Staff transfer on expiry or termination);
60.5.12 clause 28 (Parties' pre-existing Intellectual Property Rights);
60.5.13 clause 29 (Specially Created Intellectual Property Rights);
60.5.14 clause 30 (Licences of Intellectual Property Rights);
60.5.15 clause 31 (Claims relating to Intellectual Property Rights);
60.5.16 clause 37 (Official Secrets Acts);
60.5.17 clause 40 (Service Provider's Equipment);
60.5.18 clause 41 (Purchaser Property);
60.5.19 clause 44 (Tax arrangements);
60.5.20 clause 47 (Sustainability);
60.5.21 clause 49 (Warranties and Representations);
60.5.22 clause 50 (General Indemnity);
60.5.23 clause 51 (Limitation of Liability);
60.5.24 clause 52 (Insurances);
60.5.25 clause 54 (Dispute Resolution);
60.5.26 clause 56 (Waiver and Cumulative Remedies);
60.5.27 this clause 60; and
60.5.28 clause 62 (Governing Law and Jurisdiction).

60.6 If a Judicial Order is made, the provisions of the Management Arrangements referring to that possibility apply.

60.7 Immediately upon termination of the Contract for any reason whatsoever the Service Provider shall render such reasonable assistance to the Purchaser or third party nominated by the Purchaser, if requested, as may be necessary to effect an orderly assumption by a Replacement Service Provider of the Services previously performed by the Service Provider under the Contract. The Service Provider shall be entitled to charge for such termination services in accordance with Schedule 10 (Exit Management).

61 Entire Agreement

61.1 The Contract constitutes the entire agreement between the Parties in respect of the matters dealt with herein. The Contract supersedes all prior negotiations between the Parties and all representations and undertakings made by one Party to the other, whether written or oral, except that this clause does not exclude liability in respect of any misrepresentation (whether in the ESPD or Tender or otherwise).

61.2 In the event of, and only to the extent of, any conflict between the clauses of the Contract, the Schedules and any document referred to in the Contract, the following order of precedence applies:

61.2.1 the clauses of the Contract;

61.2.2 Schedule 1 (Specification and Service Levels) and their Annexes;

61.2.3 any other Schedule Parts and their Annexes; and

61.2.4 any other document referred to in the Contract.

62 Governing Law and Jurisdiction

This Contract and any disputes or claims arising out of or in connection with its subject matter or formation (including non-contractual disputes or claims) is governed by and interpreted in accordance with Scots law and, subject to clause 54 (Dispute Resolution), the Parties submit to the exclusive jurisdiction of the Scottish courts over any dispute, claim or matter arising under or in connection with this Contract or the legal relationships established by this Contract (including non-contractual disputes or claims)..

IN WITNESS WHEREOF these presents typewritten on this and the 45 preceding pages together with the thirteen Schedules annexed are executed as follows:

SIGNED for and on behalf of the Scottish Ministers	**SIGNED** for and on behalf of PeoplePlus Group Limited
At.....	At.....
On.....	On.....
Signature.....	Signature.....
Full name	Full name.....
Position	Position.....
Address.....	Address.....
In the presence of	**In the presence of**
Signature.....	Signature.....
Full name	Full name.....
Address.....	Address.....

This and the following [6] pages comprise Schedule 1 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 1

SPECIFICATION AND SERVICE LEVELS

FOR

EMPLOYABILITY SUPPORT SERVICES

FAIR START SCOTLAND

Contents

1. Introduction and Purpose of Service 50
2. The Scottish Approach to Employment Support 51
3. Equalities 52
4. Customer Suitability and Eligibility 53
5. Service Requirement 57
6. Contract Lots 58
7. Service Strands 59
8. Segmentation Tool 59
9. Service Strand Description - Core Service Strand 60
10. Service Strand Description - Advanced Service Strand 61
11. Service Strand Description – Intense Service Strand 62
12. Customer Journey 63
14. Employer Engagement 71
15. Stakeholder Engagement Strategy 72
16. Service Provider Behaviours 73
17. Branding, Communications, Marketing and Accessibility 73
18. Feedback, Suggestions, Complaints and Escalation 74
19. IT 75
20. Innovation 76
22. Outcomes not eligible as Job Outcomes 77
23. Management Information 78
24. Performance Management 80
25. Tracking Period 81
26. Monitoring and Evaluation Activities 82
27. Assurance and Fraud Team Reviews 82
28. Continuous Improvement 83
29. Service Budget and Funding Model 83
30. Payment Validation Process 84
31. Key Delivery Indicators - Validation Process 84
32. Customer Travel Expenses 85
33. Childcare Costs 85
34. Additional Costs 85
35. Open Book Accounting 86
36. Contract Management and Key Contract Milestones Dates 86
37. Contract Extension 87
38. Contract Management 87
39. Contract Review Meetings 87
40. Change Control Procedures 88

41. Mobilisation and Implementation 88
42. Data Management 89
43. Exit Strategy 89
44. Business Continuity & Disaster Recovery 89
45. Physical Data Security 89
46. Storage of Data 89
47. Risk 90
48. Sustainability, Environmental and Community Benefits 90
Annexes to the Specification 92
Annex A to Schedule 1: Sources of Information 93
Annex B to Schedule 1: Service Guarantee 94
Annex C to Schedule 1: Lots 96
Annex D to Schedule 1: Customer Volumes & Contract Values 97
Annex E to Schedule 1: Key Performance Indicators 101
Annex F to Schedule 1: Key Delivery Indicators 102
Annex G to Schedule 1: Integration and Alignment with Other Scottish Government Services 106
Annex H to Schedule 1: Additional information on Supported Businesses 107
Annex I to Schedule 1: Technical Response under separate WORD document 107
Annex J to Schedule 1: Clarifications under separate WORD document 108

1. Introduction and Purpose of Service

1.1 The Scottish Government invited tenders to deliver a new Scottish Employability Support Service, 'Fair Start Scotland', that provides support to disabled people and those at risk of becoming long-term unemployed to find and retain work.

1.2 From April 2017, the Scottish Government will implement services in line with the duty enabled by Clause 31 of the Scotland Act 2016 to provide employment support for disabled people and those at risk of long term unemployment.

1.3 As a result of these new devolved powers, the Scottish Government commissioned a one year transitional programme to support those Customers defined in the Scotland Act 2016 ("Customers"). Following the transition year, Fair Start Scotland ("the new Service") will commence from 3 April 2018.

1.4 This approach allowed the Scottish Government time to work collaboratively with stakeholders to design a new employability support service. The new Service will provide a coherent range of support that will respond flexibly to the individual needs of Customers and their employers. The Service will assist those who want to work and need help to enter and remain in work.

Designing the Scottish Employability Support Service

1.5 In summer 2015, the Scottish Government launched its consultation on devolved employability services, *Creating a Fairer Scotland: Employability Support*[1]. The aim of the consultation exercise was to draw upon the wealth of experience within Scottish communities, including the employer and provider networks to help shape future employability support in Scotland.

1.6 Following engagement with stakeholders and analysis of the consultation responses, the Scottish Government published its response: *Creating a Fairer Scotland: A New Future for Employability Support in Scotland*[2].

1.7 The Scottish Government's approach to employability is founded on the following values, underpinned by six key principles that are integral to creating a fairer Scotland.

Our Values

Value 1: Dignity and respect

Scottish Ministers are clear that Scotland's public services will be based on a culture of respect. We will have a social contract with the people of Scotland that states Scotland's public services will treat everyone with respect and dignity, and the public will treat staff providing those services in the same way. The Service will be an exemplar of this approach.

Individuals can expect to be treated with dignity and respect through each step of their journey into work.

Value 2: Fairness and Equality

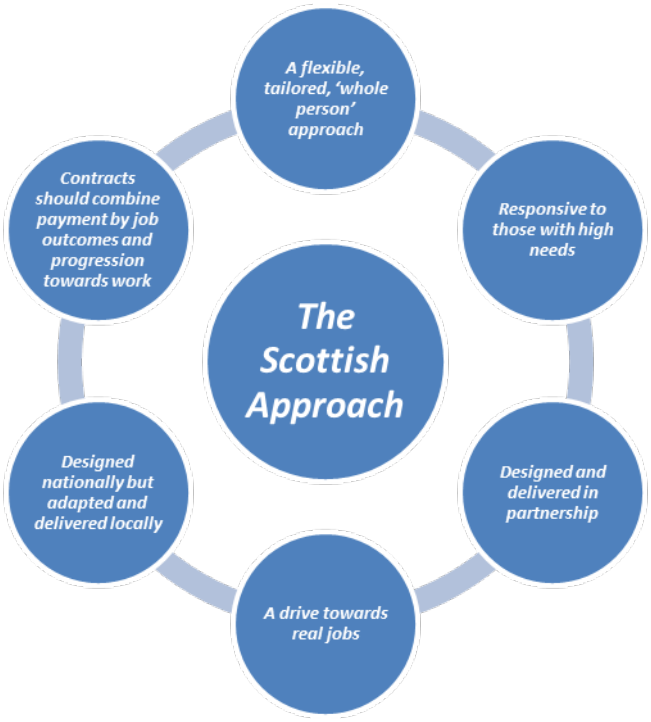
Our approach to employment support will not be driven solely by a need to reduce the Welfare Bill and focus on those with the best prospects of moving into work. Instead we will aim to contribute to a broader range of economic and social outcomes by supporting those furthest from the labour market. Customers of the Service will reflect this core value.

Value 3: Continuous Improvement

In the first instance, our priority will be to ensure a smooth transition from existing UK services to our new Scottish arrangements.

Scottish Government policies, processes and systems will evolve in response to individual, employer and community need across Scotland. The Scottish Government will ensure that they remain fit for purpose through close engagement with stakeholders and Service users alike.

Our Principles



1.8 The Scottish Government's expectation of how these values and principles can be delivered from 2018 Service is articulated through this specification. Service Providers must be clear how their provision will meet the specification and the Scottish Government's values and principles.

2. The Scottish Approach to Employment Support

2.1 The ambition to develop a distinctly 'Scottish Approach' to employment support received clear consensus and support through the 2015 consultation. The principles and values above provide the framework for this. In relation to this service requirement, the following service design elements and requirements on Service Providers are highlighted within the context of the 'Scottish Approach':

- All Customers who wish to access the Service will attend on a voluntary basis. Entirely voluntary participation creates the need for new and different relationships between referral organisations, Customers, Service Providers and Commissioners to ensure the service is both an attractive and successful support offer for Customers. The Scottish Government expects the Service Provider to be proactive in identifying, engaging and sustaining Customers in this context.

- The Service Provider will help to create a culture of dignity and respect within the Service. Having those values underpin their relationship with Customers will be the foundation on which this culture will be developed.

- All Customers must receive support which recognises their skills, attributes and assets, as well as their potential barriers to employment, with appropriate action taken to develop those individuals towards employment.

- The Service has been designed to allow the Service Provider the scope to develop personalised support for each Customer, based on their understanding of each individual and within the context of the most appropriate Service Strand for that individual. It is the responsibility of the Service Provider to build networks and align appropriate services to ensure each Customer receives the holistic support they require.

- The Scottish Approach will be underpinned by a jointly agreed Participation Agreement between the Service Providerand those participating in the Service, which will make clear the roles, responsibilities, expectations and obligations across both parties. This agreement will be underpinned by our commitment to guaranteed service levels – based on fairness, dignity and respect – and an appropriate personalised support offer.

- As the first full implementation of the Scottish Government's devolved powers on employment support, the need for continuous improvement both within the 2018 service and to inform future commissioning will be crucial and based on a partnership relationship between the Scottish Government and the Service Provider.

3. Equalities

3.1 The Scottish Government is clear in its ambitions to tackle inequality and a number of policies exist which it will be important to support through delivery of this Service.

3.2 **Disabled Employment:** At 40.9% the disabled employment rate is almost half of the non-disabled rate (81.5%) and is lower than the UK disabled employment rate of 47.9% (*ONS, Labour Force Survey, Apr-Jun datasets, 2016*)[3]. The Scottish Government has published a *Disability Delivery Plan*[4] with a series of key actions on employment and an overarching target to halve the disability employment gap. Devolved employment services will make a contribution to the achievement of this target. The Service sets out a clear focus on supporting disabled people into employment but will require the Service Provider to demonstrate a proven range of specialist skills and expertise to offer the individualised help many disabled people need to enter and sustain work.

3.3 **Women's Employment:** At first glance, women in Scotland perform well in the labour market. The current employment rate of 70.5% (ONS *Labour Force Survey June-August 2016*)[5] is the 4th highest in the EU and, since the 2008 recession, women have contributed significantly to the recovery of employment rates in Scotland – more so than in the rest of the UK.

3.4 However, occupational segregation continues to negatively affect women in terms of income levels. Caring responsibilities can mean that women tend towards lower skilled, lower paid jobs, often temporary in nature and the Scottish Government is keen to support actions to address the negative impact of such outcomes, which often lead to in-work poverty.

3.5 In line with Scottish Governments Fair Work ambitions, it is important for the Service Provider deliver a service that understands the support needs of women seeking employment. The Service Provider will use levers at their disposal to encourage employers to consider flexible working approaches which enable more women to take up a broader, more rewarding range of work opportunities. These must align with any caring responsibilities they have. The Scottish Government are seeking a gendered approach to employability support with the Service Provider supporting women into higher paid jobs in less traditional sectors.

3.6 **Black and Minority Ethnic (BME) Employment**: Some ethnic minority groups suffer disadvantage in the labour market, and when broken down by gender, the employment rate for women in these groups is even lower. There are many reasons for this. The Service Providermust engage positively to support such Customers into sustained employment, recognising the geographic variations in ethnic minority populations, and being sensitive to the cultural issues affecting them, particularly women and refugees.

3.7 **Other Protected Groups**: The Scottish Government lack robust evidence on how other protected groups are supported by employment services in Scotland and the outcomes they achieve. A clear ambition of the Service is to add to existing evidence and data on successful interventions for these groups.

4. Customer Suitability and Eligibility

Overview

4.1 Through delivery of this Contract, The Scottish Government is looking to support a minimum of 38,000 Customers' over 3 years of referrals. These Customers must be in receipt of a reserved UK out of work benefit, unless they are disabled, and will be either:

- aged 18 years old and over, out of work and living in Scotland; or
- aged 16 or 17 years old and are either disabled or in receipt of Employment and Support Allowance.

4.2 The Service will target:

- Disabled People (as defined in the *Equality Act 2010*[6]).
- Those who are long term unemployed (those reaching 2 years on Job Seekers Allowance/ Universal Credit equivalent).
- People on the Employment and Support Allowance Work Related Activity Group.
- People with convictions (someone who has completed a custodial sentence or a community sentence) or offender (someone who is completing a community sentence).
- Care Experience Young People.
- Lone Parents.
- Refugees.
- Ethnic Minorities.
- Resident in the 15% most deprived *Scottish Index of Multiple Deprivation (SIMD)*[7] areas.
- People with a health problem which presents a barrier to employment.

4.3 The Scottish Government reserves the right to amend the target Customer Groups during the term of the Contract to reflect any changes to its policies and/or priorities for employability support services in Scotland. Any amendments will be made following consultation with the Service Provider(s). Any such requirements will be subject to formal discussions and agreement according to the change control procedures detailed at Schedule 3 (Change Control Procedures).

Customer Suitability

4.4 The Service will support Customers who are significantly disadvantaged in the labour market and are assessed as having a realistic prospect of securing and sustaining work during their time on the Service.

4.5 For the majority of Customers, a realistic prospect of securing work is to be assessed by their potential to progress into work during the 12 months pre-work support period. However, for a minority of Customers, who are assessed as more disadvantaged in the labour market and

requiring additional specialist support to address their barriers, their pre-work period may be extended to 18 months with agreement from the Scottish Government.

4.6 All Customers who wish to access the Service will attend on a voluntary basis. However, Customers must be willing and able to attend regularly and engage positively with their Service Provider. The Customer and the Service Provider will agree the level and frequency of engagement during the Customer induction interview and profiling stages of the Service.

4.7 The Service will provide significant opportunities to support Customers who have a health condition and want to work. Customers will receive a range of specialised support to address the employability issues related to their health condition as described in the Service Strands requirements at paragraphs 10 and 11 of this specification.

4.8 All Customers must have their suitability for accessing the Service endorsed by their Referral Agency. Suitability must be determined by the Customer being eligible, having a realistic prospect of finding and securing work during their time on the Service, having an understanding of the Service, and being willing to engage.

4.9 The Scottish Government anticipate that the majority of Customers will be referred by Jobcentre Plus. These Customers will be identified by their Work Coach as needing more support than can be provided by the standard 'Jobcentre Plus Offer'. In all cases these Customers will have received the Jobcentre Plus core job search activity support without a successful outcome.

4.10 Additionally, other organisations operating in Scotland and supporting people who are disadvantaged in the labour market may wish to refer their clients to the Service as a next step following their own intervention. Alternatively, they may feel the Service is more appropriate for their Customers than their own support.

4.11 The *Employability Pipeline*[8] was developed in 2006 as a framework to support the effective delivery of employability services in Scotland. The Employability Pipeline sets out a 5 stage journey people may go through to enter and sustain work. The Employability Pipeline outlines the support they will require at each stage of the journey, although it also recognises that for some people, this is not a linear journey. The Scottish Government expect those referred to the Service to be in stages 2 - 4 of the Pipeline, with most being in stages 2 or 3 ('Needs Assessment and Barrier Removal' and 'Vocational Activity' respectively).

Offer to Disabled People

4.12 Disabled People, including those with severe and enduring mental health issues, will potentially access the Service, subject to suitability criteria, presenting with a wide range of issues. The Scottish Government requires specialised support to be put in place to meet all of their needs. The Service Provider must ensure that their delivery model offers a pan-disability service, offering high quality interventions for all Disabled People at all stages of their employment journey.

4.13 The Scottish Government anticipate that the majority of Disabled People will access either the Advanced or Intense Service Strands. In both these Strands, the Service Provider must offer a diverse menu of interventions appropriate to the nature of the Customer's disability. See paragraphs 10 and 11 of this specification for more information about the Service Strands.

4.14 All Customers in the Intense Strand will be taken through an individual programme of pre-work support that is consistent with the principles and practices of Supported Employment. A small number of Customers in the Intense Strand will follow the 5 stage model described in the *Supported Employment Framework for Scotland*[9], while others will be offered the most valuable elements of the model, or variations of it from a wide range of interventions. This must be discussed and agreed with the Customer.

Eligibility, Qualifying Benefits and Entry Point to the Service

4.15 Customers must be in receipt of a reserved UK out of work benefit unless they are disabled. The table below details the eligible Customer Groups, the qualifying benefits and entry point to the Service.

Customer Group	Qualifying Benefit	Entry Point to Service
Disabled People	Employment and Support Allowance (ESA); Jobseekers Allowance (JSA), Universal Credit (UC); Income Support (IS); "or no benefit at all but must be out of work".	Immediate
Health Issue placed in Work Related Activity Group	ESA, UC or Credits Only	On outcome of Work Capability Assessment.
Long Term Unemployed	JSA, UC or Credits Only	On reaching 2 years unemployed following commencement of contract.
Person with a conviction	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Care Experience Young People	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Lone Parents	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Refugees	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Ethnic Minorities	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Resident in the 15% most deprived Scottish Index of Multiple Deprivation (SIMD) areas.	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.
Unemployed but with a health condition which is a barrier to employment.	JSA, UC or Credits Only	On reaching 6 months unemployment following commencement of contract.

4.16 The Service will initially focus help towards the target Customer Groups as they cross the relevant benefit duration threshold detailed in the above table. Should participation on the

Service not meet minimum expected levels, the Scottish Government may consider extending the eligibility criteria to increase participation.

4.17 It is anticipated that the majority of referrals will come from Jobcentre Plus, who will confirm that a Customer's benefit entitlement meets the eligibility requirements for access to help through the Service through their on-going Work Coach interaction with Customers.

4.18 Customers who leave the Service during the twelve month pre-employment support period due to ill health may be re-admitted to the Service for the Balance of time. This will be at the discretion of the Service Provider taking into account the prospect of the Customer finding work during their balance of time on the Service (this measure is flexibly designed to avoid disadvantaging Customers with fluctuating health conditions).

4.19 Customers who leave the pre-employment stage of the Service early to take up work and subsequently leave for any reason will be entitled to re-join the Service for the Balance of time if the following conditions are met:

- The Customer left the job within their In-Work-Support period; and
- The Referral Agency and the Service Provider both agree that the Customers requires further support and has a realistic chance of securing new employment.

4.20 Customers whose job ends during the In-Work-Support stage of the Service will be entitled to receive support to find alternative employment up to the end of the 12 month In-Work Support period.

4.21 If the Customer moves out of Scotland and is currently within the Pre-Employment stage of the Service they are deemed to have left the Service. The Service Provider must take steps to exit the Customer, taking appropriate action as detailed within the Operational Guidance and referring to guidance regarding completion of a Leaver Plan.

4.22 If the Customer moves out of the original Lot Area to another Lot Area in Scotland and remains out of work, the existing Service Provider must continue to ensure arrangements are in place to continue to provide support to the Customer in the new Lot Area.

4.23 If the Customer is currently in work but moves out of the Lot Area to another Lot Area in Scotland, the existing Service Provider must continue to provide In-Work Support.

4.24 If the Customer is currently in work in Scotland and moves out of Scotland, but continues in the same employment, the existing Service Provider must continue to provide In-Work Support.

5. Service Requirement

Overview

5.1 The Service will deliver high quality employment support to targeted Customers' who want and need help to enter and remain in work.

5.2 The Service will provide Customers with pre-employment support for a period of up to 12 months, and In-Work support for a period of up to 12 months.

5.3 For Customers in the Intense Strand (see paragraph 11 of this specification), with significant barriers to employment, there will be the option to extend the duration of pre-employment support up to 18 months in agreement with the Scottish Government. Customers whose pre-employment support period is extended to 18 months will retain entitlement to 12 months In-Work support.

5.4 The Service will support Customers who face a range of barriers to employment: from those who may require skills, health or literacy and numeracy support; to those for whom complex barriers and/or disabilities require more specialised support to help them find and sustain employment.

5.5 The Service will be tailored to meet individual Customer needs. The Service will provide a voluntary and coherent range of specialist support that responds flexibly and effectively to meet the needs of individual Customers and their employers.

5.6 A key issue highlighted by respondents to the Scottish Government consultation on employability in 2015 was the need for a clear and consistent set of service standards that the Service Provider must deliver to every Customer.

5.7 The Scottish Government has produced guaranteed service standards (see Annex B, Service Guarantee) that set out the level of support that must be available to all Customers accessing the Service.

5.8 To support delivery of these Standards, Customers and the Service Provider must agree and sign a Participation Agreement. A template Agreement will be provided by the Scottish Government and the Service Provider must include as a minimum:

- an outline of the service offer available to the Customer;
- roles and responsibilities of both the Service Provider and Customer, setting out the commitments of each party information on the benefits of the Service;
- details of the Service Provider's complaints and feedback process, including how the Service Provider will ensure the voice of the Customer is recognised and valued in service delivery and demonstrate how this shapes provision going forward;
- information on the Service Provider's performance/success rates (which may include case studies); and
- details of the Service Provider's service delivery model and channels of engagement, and what the expected outcomes are from the Customers' perspective. The Service Provider must note that the Scottish Government requires minimum core hours for the Service to be Monday to Friday 0900 – 1700, except on statutory public holidays.

5.9 To ensure the Service offers the most effective support possible to Customers, a number of key features need to be integral to its delivery. The Service Provider must:

- demonstrate innovative approaches to working with those with more complex support needs;

- deliver support for the Customers to enable them to achieve their potential, whilst ensuring the Customer retains full choice and control over the support that they receive at all times, within the Service Strand to which they are allocated;

- ensure all elements of their agreed service are accessible across the whole Lot and provide the Guaranteed Service of support for Customers as outlined in Annex B;

- actively promote the new Service to potential Customers and Referral Agencies, promoting integration and alignment with local organisations and stakeholders to support the effective delivery of the Service;

- identify partner organisations to deliver specialist provision to meet the needs of the diverse Customer Groups and work closely with others, e.g. health and/or social care organisations, to identify Customers who may benefit from the Service;

- build strong links with local employers to encourage participation in the delivery of the Service;

- operate a quality feedback process for Customers and their employers throughout the Customer employment journey;

- promote the Scottish Government's ambitions around Fair Work, payment of the *Scottish Living Wage* [10] and support the Scottish Government's Diversity and Equality Policy [11] to supply chain/ consortia partners and the employers that they work with; and

- ensure that Service Provider staff and their supply chain are checked to the appropriate disclosure level. Advice should be sought from Disclosure Scotland if required.

6. Contract Lots

6.1 The Service will be delivered across nine (9) geographical Lots based on clusters of Scottish Local Authority Areas. This offers a mix of viable contract sizes which the Scottish Government has awarded to a diverse range of Service Providers.

6.2 In line with Regulation 21 of the Public Contracts Scotland Regulations (2015), Scottish Ministers decided to reserve one Lot for supported businesses. The Scottish Government is committed to furthering the development of supported businesses in Scotland.

6.3 A Supported Business is defined in the Public Contracts (Scotland) Regulations 2015 as:

> *"an economic operator whose main aim is the social and professional integration of disabled or disadvantaged persons and where at least 30% of the employees of the economic operator are disabled or disadvantaged persons;"*

6.4 Lot: 'West' (covering the East Dunbartonshire, East Renfrewshire, Inverclyde, Renfrewshire and West Dunbartonshire Local Authority areas) is reserved.

6.5 All references to Lot: 'West' in this Specification are for information purposes only.

6.6 A single contract was awarded for each Lot. Further information about the Lots are included at Annexes C and D to this Schedule.

6.7 The Service must be available and accessible to all Customers living in the Lot. The Service Provider will be required to deliver the proposed provision from premises located within the relevant Lot. Customers will be resident in various areas across each Lot and so the delivery premises should be sited in locations which are accessible via public transport. The Service

Provider will be required to provide details of proposed delivery premises, including a rationale in support of their proposals.

7. Service Strands

7.1 The Service offer to Customers will be categorised by one of three Service Strands. The Scottish Government will provide a standardised Segmentation tool to assist in determining the Service Strand required by each Customer.

7.2. The assignment to the Core, Advanced or Intense Service Strands, as described below, will determine the level of support available to the Customer during their employment journey.

- **Core Service Strand** – for Customers who require a range of support to overcome barriers to work;

- **Advanced Service Strand** – for Customers who face more significant barriers to work and require specialist interventions and support; and

- **Intense Service Strand** – for Customers with multiple and more complex needs, and significant barriers to work, that require the support of dedicated specialist organisations.

7.3. The Service offer within each Strand is driven by the primary relevant barriers and the expected target Customer groups. However, the Service offer must be personalised and tailored to the needs of the individual Customer.

7.4. In line with the Scottish Government's core values, Customers, Service Provider staff, Consortium and/or Supply Chain partners and Stakeholders must always be treated with dignity and respect. As such, the Service Provider must refrain from using the Service Strand terminology or jargon with Customers.

8. Segmentation Tool

8.1 The Scottish Government wishes to ensure that every Customer is allocated to the Service Strand which provides the level and intensity of support that their barriers to employment require. It is anticipated that the Service Strands will therefore have different financial values to recognise the escalating need across the Customer groups.

8.2 The only purpose of this tool is to assign Customers who have voluntarily agreed to join the Programme to one of three Service Strands. The three Strands are:

a) Core
b) Advanced
c) Intense.

8.3 The Segmentation tool is *not* a full diagnostic of the needs of the Customers nor is it intended to be.

8.4 Every Customer who starts on the Programme must have completed the Segmentation Tool to determine the level of their needs and barriers to employment. It will be the responsibility of each Service Provider to ensure that every Customer has completed this activity in advance of starting on the Service.

8.5 The Service Strands are therefore a key driver of both the nature of the support given to a Customer and for the performance of the Programme (as measured by job outcomes). Making sure each Customer is assigned to the correct Strand will be critical to the success of the Service.

8.6 The Scottish Government is currently developing this tool and will 'test' this model prior to the Service commencement date. The Scottish Government will work closely with the Service Providerto ensure it operates correctly.

9. Service Strand Description - Core Service Strand

9.1 It is anticipated that Customers in this group will mostly be unemployed and job seeking and will be a mix of some Customers in the early entry categories (namely, Lone Parents, Care Leavers etc.) and some who have reached the 24 months unemployed stage. They will face barriers to work which might include a skills deficit, literacy and numeracy problems, and a lack of confidence and resilience. They may also face some 'environmental' barriers such as travel and childcare. The Scottish Government do not expect most of those with a disability or a health condition acting as a barrier to work to be in this Service Strand.

9.2 The Service Provider must provide Customers with a dedicated advisor and a range of activities that are tailored to individual Customers and their needs. The activities must build on the service outlined in the Guaranteed Service Standards. The level of activity and engagement will increase steadily during the time on the Strand to prepare the Customer for the world of work.

9.3 The level of activity and rate of increase in hours must be determined, agreed and recorded by the Service Provider and the Customer, and must recognise any benefit conditionality. Operational Guidance will provide further detail.

9.4 The Service Provider is encouraged to propose innovative delivery proposals for enhancing the Customer experience during this phase. Given the voluntary nature of the Service, Customers will need to be enthused to engage on a regular basis. The Service Provider may want to consider some form of Group activity that promotes collaborative engagement with Customers.

9.5 Detailed below are support activities that must be offered to Customers in this Strand. This is not an exhaustive list, and the Service Provider must determine the range of support available to reflect Customer needs:

- a mix of **one to one support and group work** with the expectation that individual's progress to intensive job search at an early stage. Depending upon Customer need, group work may include activities that promotes team-building; and develop the skills/attributes required in the workplace (e.g. interpersonal skills, communication skills, leadership skills etc.);

- **core employability support** from a dedicated adviser that builds upon services/interventions already received by the Customer from JCP or other specialist employability organisations (e.g. confidence/resilience building, preparing for interviews, job matching and brokerage);

- **employer presentations** – presentations from local employers about working in specific employment sectors e.g. retail, hospitality, business admin and manufacturing. This may cover how to get a job in a particular sector, application processes, recruitment practices (e.g. on-line job applications and questionnaires/psychometric testing etc.);

- **intensive job search**, including digital job search techniques, and the use of the internet/registrations with job sites/agencies etc.;

- **job application support** – including CV and interview preparation, skills development, managing disclosure of health/disability/conviction information, and advocacy to the employer if needed;

- **personal development** – improving self-esteem, addressing any issues with confidence, motivational, resilience and attitude;

- support from **a mentor**;

- **vocational or employability skills training** appropriate to Customer's job aspirations where it would remove a barrier to work;

- **volunteering** opportunities;

- **work experience/placements** – short work experience/placement opportunities with employers; these are expected to last between 4-6 weeks. This type of activity must recognise any benefit conditionality requirements; and

- support for Customers wanting to enter **self-employment**.

10. Service Strand Description - Advanced Service Strand

10.1 It is anticipated that these Customers will be a mix of; long term unemployed joining the service at 24 months; a smaller number of early entry unemployed people (for example Lone Parents, Care Leavers etc.); some disabled people and those in the Employment and Support Allowance Work Related Activity Group. In addition to the range of possible barriers faced by those in the Core Strand, they will possibly face a number of additional challenges. These might include: a long-term health problem which is acting as a barrier to work; in recovery from addictions; a record of convictions and/or other non-employability related issues, such as housing difficulties.

10.2 The Service Provider will provide Customers in this Strand with all appropriate support available to those in the Core Strand. In addition further specialist support such as is listed below must be available. This list is not exhaustive.

- **Access to specialist support to address health problems**. This must include professional help to manage mental/physical health conditions and well-being interventions. The Service Provider may wish to make Cognitive Behaviour Therapy or other forms of condition management available;

- **Support to find work while in recovery from drug/alcohol/substance misuse;**

- **Support to develop skills for the workplace**; and

- **Support to address the barriers faced because of a record on convictions.** This may include guidance on matters of disclosure.

10.3 It is the responsibility of the Service Provider to build networks and align appropriate services for each Customer to ensure they receive the holistic service they require as set out earlier in this document. The Scottish Government anticipate that this will be particularly applicable to those Customers in the Advanced Strand.

10.4 Therefore, in addition to the services above, and the specific needs of the Customer, the Service Provider may signpost/make a warm referral to other agencies and Scottish Government funded programmes where agreed with the funding body, including areas such as addiction services, housing support and childcare advice. Access to these initiatives is subject to a range of criteria and will, in some cases, be limited by the availability of places. The Service Provider is expected to negotiate with other local organisations to allow Customers to access these initiatives, if appropriate.

10.5 Some Customers who have a disability will be assessed as not requiring the high level of support available through the Intense Service Strand, and instead will be supported in the Advanced Strand. The Service Provider will have knowledge of their Customers with a disability and their likely barriers to employment. The Scottish Government would expect that:

- Disabled Customers in the Advanced Strand can expect to receive high quality, personalised one-to-one support with specialist provision where required;

- Disabled Customers will receive high quality assessment and action planning (although not necessary a full Vocational Profile); and

- Disabled Customers in the Advanced Strand must also receive Job Analysis, high quality In-Work Support and have an In-Work Action Plan.

10.6 The Scottish Government expect the level of activity and engagement to increase steadily during the time on the Strand to prepare the Customer for work. The level of activity and rate of increase in hours will be determined between the Service Provider and the Customer.

11. Service Strand Description – Intense Service Strand

11.1 It is anticipated that this Customer group will predominantly be disabled people. Others with long-term health conditions such as severe and enduring mental health conditions may not consider themselves disabled but may be judged by the Segmentation Tool as requiring this Intense Strand of support.

11.2 Others who face multiple and complex barriers to work may require this level of support. They are likely to have a poor or limited employment history, or have been out of work for 5 years or more and will face a range of barriers to work noted in the Core and Advanced paragraphs of this Schedule in addition to a disability and / or long-term health condition.

11.3 The service will be built on the principles of the Scottish Government Supported Employment Framework, and although not all Customers will follow the Framework, they can all expect a service including key elements of supported employment:

- All Customers will receive end to end and 1:1 support from a specialist key worker who has a sound knowledge of their disability and their barriers to employment.

- The Service Provider is required to ensure that staff involved in the delivery and management of this proposed support are appropriately qualified and/or experienced in delivery of Supported Employment services. The Service Provider is, therefore, required to provide information about the qualifications and experience of staff, together with an explanation of why they believe these to be appropriate in the context of the proposed provision.

11.4 All Customers must be offered Vocational Profiling, conducted to the best standard principles of person-centred planning and also include information on skills, attributes, aspirations, past experience, health and social issues, communication needs and how support will be delivered. This will be used to develop an action plan which will detail the activities to be carried out to prepare the client for employment.

11.5 Those in the Intense strand will require an enhanced level of support and there is an expectation that Customer to advisor ratios will be much lower in this group. It is recognised that there are practical challenges around setting a Key Delivery Indicator for this against which the Service Provideris measured, but evidence has shown that a Customer to Advisor ratio of 1:20 is appropriate. Independent advocacy support must be arranged where the Customer requests this.

11.6 The Service Provider must provide a range of activities that are tailored to individual Customers and their needs. The activities must build on the service outlined in the Guaranteed Service Standards. The Scottish Government expect the level of activity and engagement to increase steadily during the time on the Strand to prepare the Customer for

work. The level of activity and rate of increase in hours will be determined between the Service Provider and the Customer.

11.7 The Service Provider is expected to provide Customers in this Strand with all the support provided to those in the Core and Advanced Strands. In addition, the Service Provider will provide the following to the Customers in the Intense Strand (as before, this is not an exhaustive list) and the Service Provider must determine the range of support available to reflect Customer needs:

- Models including the Supported Employment Model for disabled people and Individual Placement and Support (IPS) for those with severe/enduring mental health challenges must be available and offered where required.

12. Customer Journey

12.1 The Scottish Government does not wish to be overly-prescriptive in terms of service content as this must be tailored to each Customers individual circumstances, their job aspirations and the needs of the local labour market. However, the Service Provider must follow the high level Customer Journey Stages set out in this specification.

12.2 Additionally, the Service Provideris required to observe and comply with any Operational Guidance which is issued by or on behalf of the Scottish Government during the Contract period. This guidance will be limited to administrative matters and will be considered for commercial impact on the Service Provider before issue. Where a change is considered significant it will be subject to discussion with Service Provider and subject to formal Change Control (see Schedule 3 (Change Control Procedures)) where the Service Provider considers this necessary.

12.3 Existing support funded through the Scottish Government to support skills development has been considered and Annex G sets out how the Service will align with these initiatives.

Stage 1: Pre Start – Identification and Referral

The Scottish Government anticipate the Service will attract referrals from a wide range of organisations across Scotland such as:

- Jobcentre Plus (JCP);
- Local Authorities;
- Third Sector organisations;
- Social Service Teams;
- Carer Groups;
- Education & Learning institutions; and
- The National Health Service / Health Scotland.

This list is not exhaustive.

The Referral Agency will provide the Customer with a brief overview of the Services offered by the Service Provider, the features and benefits of the Service, what support is available, and the location of the Service Provider's local offices. The Service Provider will provide their own marketing material to assist Referral Agencies with this step (see paragraph 17 for further information).

The Referral Agency should ensure the Customer's suitability for accessing the Service is agreed with the Customer prior to the Stage 2: Eligibility Check.

Stage 2: Eligibility Check

It is anticipated that JCP will be a primary source of referrals, and that all Customers in receipt of working age benefits, will have their eligibility checked via their on-going interaction with their JCP Work Coach, using the Service eligibility criteria, before being referred to the Service.

In instances where a referral is made to the Service Provider for Customers in receipt of working age benefits by an organisation other than JCP, the Service Provider must signpost the Customer back to JCP to ensure that the Customer's Work Coach actions the referral to the Service.

In a small number of cases, there may be eligible Customers for Fair Start Scotland who have no requirement to engage with Jobcentre Plus, either as they are not in receipt of benefit or their benefit conditionality does not require this. For this Customer group, a clerical referral can be made by the Referral Agency direct to the Service Provider, who will check eligibility. Details must be recorded in the Customer case file to confirm this action has been undertaken.

Full details of these processes will be shared through the Operational Guidance.

Stage 3: Referral Process and Warm Handover

The Scottish Government recognises that the ability to support warm handovers will depend on local arrangements, and relationships built between the Service Provider and their range of Referral Agency partners.

Where warm handovers can be supported, the Referral Agency will be responsible for contacting the Service Provider to arrange a 'warm handover' for the Customer. The Referral Agency, with the Customer's consent, will contact the Service Provider to discuss the referral details and Customer circumstances in advance of the warm handover.
The purpose of the warm handover is to:

- encourage effective working between the Referral Agencies and the Service Provider;
- improve the standard of referrals, in terms of appropriateness of referral and background information provided;
- establish the Customer's willingness to engage with the Service;
- enable a collective assessment between Customer, Referral Agency and Service Provider of the support needs of the individual; and
- agree a start date with the Customer to commence the Programme.

The warm handover meeting, attended by the Customer, Service Provider and Referral Agency, is expected to last up to 1 hour. The Customer must be made aware of the purpose and content of the meeting in advance of attending.

Preferably, the warm handover will be done face-to-face but it may be completed by telephone, Skype, etc. depending on local arrangements agreed with the Service Provider and the Referral Agency. Any travel costs incurred by the Customer will be the responsibility of the Service Provider.

At this stage the Customer may deselect themselves from further involvement in the Service. The Service Provider must notify the Referral Agency that the Customer has declined the offer of support.

The Service Provider will not have the option to reject referrals. Information about how to advise the Scottish Government of inappropriate referrals will be included the Operational Guidance.

Once the Customer agrees to engage with the Service, the Referral Agency will make a referral to the Service Provider. This is the date at which the Customer is referred to the Service. The Service Provider must confirm with the Referral Agency that the Customer has agreed to commence the Service and confirm their start date.

The Service start date and time (i.e. the induction interview appointment) must be no more than 5 working days, following receipt of the referral by the Service Provider. In exceptional circumstances and due to reasons out with the Service Providers control where this timescale cannot be met, the Service Provider must annotate the Customer file accordingly explaining the reason for the delayed start.

Stage 4: Pre Start

Immediately following the warm handover, the Service Provider must notify the Customer and Referral Agency in writing of the date and time for their Induction Interview, and follow up with a courtesy telephone call 48 hours prior to this appointment to alleviate any Customer concerns.

Prior to their Induction Interview with the Service Provider, the Customer must complete a Self-Assessment to determine the most suitable Service Strand for them. Should the Customer need help to complete the Self-Assessment, the Referral Agency should arrange this support.

The Self-Assessment will be undertaken by using the Segmentation Tool.

Stage 5: Service Start - Customer Induction Interview

The Service Provider has the discretion to determine the most appropriate format for managing and delivering Customer Induction Interviews. The only stipulations are that the interviews must be conducted face-to-face and within 5 working days of the initial Customer referral being received. If the Customer is unable to ‘start’ on the date offered, the Service Provider must record on file.

The purpose of the Induction Interview is to:

- outline the service offer;
- outline the roles and responsibilities for both the Service Provider and Customer and jointly sign a Participation Agreement, setting out the commitments of each party;
- introduce the Customer to their named key worker who will be responsible for providing continuity of support throughout the employment journey;
- provide an initial assessment to inform the Customer Profiling and Planning Stage (see Stage 6) of the Service; and
- discuss Customer participation in evaluation activities.

At the Induction Interview, the Service Provider must provide each Customer with an Induction Pack. As a minimum, this must include:

- Background of the Service Provider;
- What the Service offers;
- What happens next;
- Who are the Customer’s key contacts;

- Details of Service Provider's Customer Charter and Complaints/ Suggestions procedures;
- Health and Safety requirements; and
- Other useful information – website details, success stories, information security, etc.

The Service Provider is encouraged to propose innovative delivery proposals to support and retain the commitment from the Customer. This must enhance the Customer experience throughout their participation on the Programme. Given the voluntary nature of the Service, Customers will need to be enthused to engage on a regular basis. The Service Provider will want to consider some form of group activity that promotes collaborative engagement with Customers from initial engagement through their time on the Programme.

The Service Provider must facilitate immediate referral to specialist services following the induction interview for Customers identified as having complex and significant barriers to work who require support provided through the Intense Service Strand. The specialist services organisations will be responsible for undertaking the Customer profiling and assessment activities.

Stage 6: Customer Profiling and Planning Activities (Week 1 to 8)

Once the Customer starts on the Programme, the Service Provider will undertake profiling and planning activities. The activities will be split into two parts:

Weeks 1 to 3

During the first three weeks the Service Provider must engage with the Customer to:

- assess their needs, identify barriers and job aspirations;

- review their completed self-assessment to confirm the service strand they will access; and

- confirm the level of support offered to the Customer determined by the appropriate Service Strand.

Weeks 4 to 8

The Service Provider will use the balance of time during this Stage of the Service to confirm the appropriateness of the allocation to the Service Strand.

There may be instances where the Service Provider considers that the original allocation to the Service Strand is wrong and, following observations and discussions during the activities outlined above, wishes to change the Service Strand. In exceptional circumstances and with the agreement of the Scottish Government a change to Service Strand may be approved. The process for this will be outlined in the Operational Guidance.

During this period the Service Provider must offer the following:

- Weekly interventions with the Customer's key worker;

- Access to a range of essential activities that will help to determine/confirm the level of help and support required, including but not limited to:

    - baseline development of employability skills;

    - health and well-being assessments and guidance;

    - jobsearch skills and resources;

    - labour market information, including employer engagement;
    - mentoring support;
    - money management;
    - personal development and soft skills training, e.g. communications and interpersonal skills;
    - promotion of IT for job search (including assessment of IT skills);
    - social activity to support the engagement and development of soft skills;
    - understanding the world of work – employer presentations; and
    - volunteering opportunities.
- development of a detailed personalised Employment Action Plan which sets out agreed activities and timescales for helping Customers into work. This will include: an assessment of current skills; employment history, vocational training needs; employment aspirations; agreed activities for overcoming barriers to employment, including engagement with external services; and monitoring and review arrangements and In-Work Support plan;
- identification, referral and support for the Customer to engage with specialist organisations to provide appropriate support to address issues;
- the opportunity to fast-track Customers to specialist organisations to provide appropriate support; and
- Customers with the highest support needs (i.e. those referred to the Intense Strand) will receive a Vocational Profiling service that supports their individual Action Plan during this period.

The Service Provider is required to propose innovative delivery proposals for enhancing the Customer experience during this phase.

Stage 7: Intervention and Customer Engagement (Weeks 9 to 52)

By week nine, Customers will commence in one of the three Service Strands. The Customer will continue to receive a range of core activities (listed at Stage 6), supplemented by more targeted and/or specialised interventions that address their needs and employability issues. The level of activity and engagement must increase steadily during the time on the Strand to prepare the Customer for the world of work.

To support the Guaranteed Service, the Service Provider must provide the following support during this stage of the employment journey:

- minimum of 3 hour face-to-face contact with named key worker per week;
- 1 to 1 coaching by the named key worker, as necessary;
- formal face-to-face monthly review with the named key worker;
- quarterly distance travelled assessment and feedback with the named key worker;
- employability activities as detailed in the individual Employment Action Plan;

- engagement with external, specialist or partner services as detailed in the individual Employment Action Plan;

- access to work experience opportunities and appropriate monthly workplace reviews;

- weekly job search activities;

- employer engagement, including support for interviews and negotiations of reasonable adjustments; and

- financial guidance.

Evidence of pre-employment activity and support must be recorded in individual Customer files and Action Plans which will form part of the monthly performance management process between the Service Provider and the Scottish Government.

If a job outcome is not achieved during this timeframe, the Service Provider will produce a Leaver Plan and refer the Customer back to the original Referral Agency.

In exceptional circumstances and due to unacceptable Customer behaviour, a process will be established to exercise an option to cease provision of Services. This process will be fully outlined within the Operational Guidance.

Service Provider Case Conferencing with Referral Agency

- It is considered good practice for the Service Provider to maintain contact with the Referral Agency to provide regular updates on those Customers they have referred to the service. Scottish Government would encourage arrangements to be put in place for Case Conferencing where appropriate to discuss the Customer's progress. These will mainly be done on an individual basis face to face or by conference call. These can also be conducted as part of a wider group session where deemed appropriate by the Service Provider and the Referral Agency.

Disengagement

- If the Customer disengages or becomes inactive, e.g. fails to attend appointment or participate in an agreed activity without prior notice, the Service Provider must contact the Customer within 24 hours to establish the circumstances surrounding the disengagement.

- If the Service Provider is unable to engage with the Customer within 5 working days of them failing to attend an appointment/activity they must contact the Referral Agency to ascertain the circumstances for this (focusing on known barriers and/or risks) and agree an appropriate way forward to re-engage the Customer.

- If the Customer disengages or becomes inactive on 3 separate occasions it is for the Service Provider to determine whether the Customer should continue to participate in the service. Service Providers are responsible for determining the most appropriate course of action. Full details of this process will be contained within the Operational Guidance.

- Should the Customer be dismissed from the Service, the Service Provider must record the reasons for dismissal within the Customer's Leaver Plan.

Stage 8: Customer does not find work during the 12 month pre-employment support period (Intense Service Strand Customers' only)

Only Customers in the Intense Service Strand who fail to secure employment following completion of the 12 month pre-employment support period may have the option to extend the

pre-employment support. This can be extended to a maximum duration of 18 months, where Customer and Service Provider are agreed that there is a realistic prospect of the Customer finding a job in this timescale. Customers whose pre-employment support period is extended to 18 months will retain entitlement to 12 months In-Work support.

If there is no, or limited prospects of the Customer finding work within the 6 month extension period, the Service Provider must engage with the Referral Agency within 10 Working Days of Customer's end date to arrange for the Customer to be referred back. This is to ensure a smooth transition back to the Referral Agency and must be supported with a detailed Leaver Plan (in accordance with stage 9 below).

Stage 9: Service Exit and Leaver Plan

Customers failing to secure employment within 12 or 18 months (see stage 8 above re extensions) will be referred back to the Referral Agency responsible for the original introduction. The Service Provider must contact the Referral Agency prior to the Customer's end date to alert them that the Customer will be returning.

The Service Provider must produce a detailed Leaver Plan for each Customer returning to their Referral Agency. As a minimum, the Leaver Plan must include the following:

- identified barriers to employment, for example: addiction; and/or vulnerability issues;
- distance travelled, for example: new learning; basic skills; and learning and development activities;
- activities undertaken whilst on the Service;
- reason for leaving provision; and
- recommendations on next steps to support Customer move closer to employment.

The exit process and Leaver Plan applies to all Customers disengaging from the Service and returning to their Referral Agency. Those who, for any reason, do not enter work but do not complete the Programme, will be referred back to their Referral Agency for consideration of further support.

Stage 10: In Work Support (13-24 months, or job entry date + 12 months)

Once a Customer has found paid employment (or self-employment), the Service Provider will work with the employer and Customer, as appropriate and determined by the Customer, to identify the support required for the Customer to start and retain work. Thereafter the Service Provider will provide a period of In Work Support, which has the ambition of supporting job retention/ progression in terms of skills and / or income. Careers Information Advice and Guidance may be suitable at this stage.

In line with the funding model, the Scottish Government would not expect the total period of In Work Support to exceed 12 months.

The Service Provider will need to be fully conversant with the range of support that can be made available, and this information must be detailed within the Customer's In Work Support Plan.

Subject to the Customer's agreement, the Service Provider is required to support them to retain employment or secure new employment in the event of the Customer becoming unemployed before the 12 months in-work support period is complete.

The Service Provider is required to:

- facilitate within 10 working days of job start date, a jointly agreed In-Work Support Action Plan, detailing timeline for workplace reviews with employer, future training and career development goals and actions;

- support the workplace induction;

- provide a minimum of weekly contact with the Customer fading as appropriate;

- conduct monthly workplace reviews with the employer, reducing over time as appropriate;

- support at workplace training (if necessary);

- provide support to develop workplace relationships;

- provide financial guidance, including advice for their employer, training for employer's staff (as necessary);

- ensure the Customer is aware of any changes to their benefit entitlement and ensure that they are receiving all appropriate in work benefits by sign-posting them to JCP for expert advice;

- if appropriate, ensure the Customer is aware of their rights as a disabled person (as defined by the Equality Act 2010);

- liaise with the Access to Work Specialist Advisory Team, where appropriate, to provide advice and support about accessibility solutions; and

- conduct individual exit planning in the final stages of the Programme.

In addition, for Customers in the Intense Service Strand, the Service Provider must provide:

- Job Analysis and Task Analysis. Customers will be offered In-Work Support specific to their particular needs. Job Analysis must be undertaken for each Customer entering employment to inform the In-Work Support Action Plan, which, with Customer consent, must be agreed with the employer. For Customers who have been supported through the Supported Employment Framework this will also include a description of the job coaching they are receiving and a plan for withdrawing this support over time; and

- those following the Supported Employment Framework can also expect job-coaching, reducing over time as appropriate

Within this Specification, the Scottish Government has provided detailed service requirements both at a Service level and in relation to the 3 Service Strands of Core/Advanced/Intense.

13. Partnership, Integration and Alignment

13.1 The approach to delivery set out in this Specification will require the Service Provider to build and maintain excellent working relationships with key stakeholder organisations and groups to help provide effective and joined up support for Customers. These include but will not be limited to:

- The Scottish Government;
- Customer Representative Groups;
- Jobcentre Plus;
- Local Authorities;
- Skills Development Scotland;
- Third Sector Employability and Specialist Service Organisations;
- Centres for Independent Living;

- Integration Joint Boards (Health and Social Care);
- Employers (in the public, private and third sectors);
- Social Service Teams and Organisations;
- Carer Groups;
- Organisations that represent the interests of disabled people with a disability (e.g. user groups);
- Education and Learning Institutions;
- NHS e.g. Mental Health Support Teams;
- Healthy Working Lives Centres;
- Alcohol & Drug Partnerships;
- Organisations that represent the interests of people with convictions; and
- Organisations working in Homelessness.

13.2 The Scottish Government has a long standing ambition for greater integration and alignment across public sector delivery. Devolution of employment services provides an opportunity to not only build on the strengths of existing national and local services but to develop a long-term plan that will set out the Scottish Government's vision for achieving greater alignment and integration.

13.3 Building on existing good practice, effective engagement with such partners (at an appropriate level) will help to ensure that services recognise and reflect local needs, priorities, strategies and resources to achieve best outputs and value for money, and offer a comprehensive service that meets the needs of all Customers.

13.4 The Service Provider is required to take into account local initiatives and publically funded services to support an agenda to improve performance and the quality of support to individuals, reduce duplication of spending by public sector bodies and improve the effectiveness of the use of public funds in the locality in which services are being provided.

13.5 The Service Provider is required to work closely with such partners and accept working with such partners is a service requirement.

13.6 As part of on-going quarterly Contract reviews, the Service Provider is required to discuss their efforts to encourage partnership, integration and alignment. This extends to the sharing of good practice, challenges and risks across the Lot.

13.7 In addition, the Service Provider is required to participate in 6 monthly Scottish Government led employment services 'share and learn' events at a national level, to share best practice, data, what works, etc.

14. Employer Engagement

14.1 To achieve high levels of good quality job outcomes, employer engagement will be key to the success of the Service. The Scottish Government will actively work with the Service Provider and other stakeholder/partners to ensure high quality employer engagement which addresses:

- the need for the Service Provider to have a strong understanding of existing and emerging labour markets across the Lot;

- the need wherever possible to align with local and national employer engagement strategies or plans to avoid duplication;

- the development of mutually beneficial relationships with employers which enable the Service Provider to influence employers positively in terms of the staff they recruit on the basis of business benefits that can be accrued; and

- links to existing Scottish Government policies, including the Scottish Business Pledge, Fair Work ambitions, and efforts to tackle inequality and occupational segregation.

14.2 Scottish Government expects the Service Provider to engage with employers by demonstrating that the Service is designed to better meet their recruitment needs by including substantial employer involvement, which offers Customers:

- first-hand information relating to the world of work;
- the opportunity to discuss 'what makes a successful employee' with employers;
- the opportunity to undertake job interview practice with a local employer;
- awareness of 'first impressions' – dress to impress and personal hygiene;
- visits to local employer premises;
- short work experience opportunities; and
- the opportunity for Customers to discuss issues with existing employees.

15. Stakeholder Engagement Strategy

15.1 The Service Provider must develop, deliver and maintain a Stakeholder Engagement Strategy ("the Strategy") to reflect how the Partnership, Integration and Alignment and Employer Engagement requirements will be met.

15.2 The Strategy must be supported by a detailed Stakeholder Engagement Plan which outlines the Service Provider's approach to engaging, working effectively and collaboratively with the external stakeholders to maximise Customer outcomes.

15.3 The Scottish Government will require Service Providers to refine their Stakeholder Engagement Plan with the Scottish Government prior to the Service Delivery 'Go live' date of the contract and progress will be monitored at the monthly Contract Performance Reviews.

15.4 The Stakeholder Engagement Plan must clearly describe how the Service Provider will achieve greater integration with existing local services and health provisions and must include as a minimum: the interventions, timelines/ frequency of engagement, delivery methods of engagements and communications with the broad range of local stakeholders and support services.

15.5 The Stakeholder Engagement Plan must explicitly detail how the Service Provider will engage and work with employers to a) allow employers to feed into the Service design and delivery b) support and encourage employers to employ Customers using the Service.

15.6 As part of on-going quarterly Contract Performance Reviews, the Service Provider is required to discuss their efforts to encourage partnership, integration and alignment. This will extend to the sharing of good practice, challenges and risks across their Lot.

15.7 The Service Provider will be required to provide an updated Stakeholder Engagement Plan every three months. The Stakeholder Engagement Plan and any amendments to it will be subject to the approval of the Scottish Government.

16. Service Provider Behaviours

16.1 In line with the Scottish Government's principles and values, where the Service Provider sub-contracts, enters into partnership agreements or forms consortia for the Service delivery, they must:

- be committed to achieving the best possible outcomes for its Customers;
- act with integrity in their dealings with these parties;
- ensure transparency, non-discrimination, equal treatment and clearly defined accountability in relationships between parties;
- encourage the sharing of good practice;
- agree, document and abide by the terms of delivery and funding at the outset;
- agree monitoring and management information requirements that are not overly bureaucratic and must be consistent, proportionate, clearly specified and agreed at the Effective Date;
- develop and support its sub-contractors or partners to improve overall supply chain effectiveness;
- agree and deliver a level of support for all parties; in particular any new entrants into the market; and
- be transparent about decisions or referrals of Customers to delivery partners including the level and type of support needed.

17. Branding, Communications, Marketing and Accessibility

17.1 While the Scottish Government will actively market the Service prior to the service start date, the Service Provider- is also required to pro-actively market and promote the Service, reaching out and engaging Customers who may not have previously accessed available employment support once the Service has commenced.

17.2 Given the voluntary nature of the service, the Service Provider must develop innovative and effective communications and marketing activities to attract Customers and enthuse them to engage and attend on a regular basis.

17.3 The Service Provider will be required to use the agreed Scottish Government Branding for the Service (which is owned by the Scottish Government). The Branding will be provided to the Service Provider on the Effective Date.

17.4 The Service Provider shall ensure that the Fair Start Scotland name and branding is included on all communications (including promotion and marketing material) relating to the delivery of the Service.

17.5 The Service Provider must ensure that dedicated feedback inbox details are given to Customer and promoted/displayed on marketing leaflets and public areas of Service Provider's premises.

17.6 The Service Provider must note that the following domain names belong to the Scottish Government:

- fairstartscotland.co.uk
- fairstart.org.uk
- fairstartscotland.org.uk
- fairstartscotland.uk
- fairstartscotland.com
- fairstartscotland.org
- fairstart.scot
- fairstartscotland.scot

17.7 The process and guidelines for use of the Scottish Government Logo and Fair Start Scotland Logo are detailed in the Operational Guidance.

17.8 All communications (press releases, announcements, advertising, publicity material or activity and similar such communications) associated with the operation of the Service must be submitted to the Scottish Government for approval. The Service Provider must not issue any communications until written/email confirmation is received from the Scottish Government confirming that the communication is approved and can be issued.

17.9 The Service and all its content, notices, templates, forms, marketing material and associated services must be provided in English. If required, the Service Provider must make documentation available in other languages, in audio format, in Braille, large print and in other formats.

17.10 Access to portals and associated documentation must be comprehensive, clearly laid out and be easily understood by all users.

17.11 All Customer user guides must be assessable to users with visual or other disabilities and be compatible with industry-standard screen readers or other assistive technology (compliant to Level AA of the Web Content Accessibility Guidelines (WCAG) / ISO 40500:2012 or equivalent).

18. Feedback, Suggestions, Complaints and Escalation

18.1 The Service Provider must operate a quality feedback process for Customers, ensuring the voice of the Customer is recognised and valued in service delivery and demonstrates how this shapes provision going forward, ensuring systems are in place to encourage Customers to feedback on their experience of the Service. This must include suggestions for improvement; positive feedback and complaints.

18.2 For complaints, the Service Provider must put in place an internal dispute resolution procedure to deal with issues raised by Customers regarding the delivery of this Service. This must include clear and reasonable timescales as detailed below for resolution and a defined escalation process. The Service Provider must acknowledge receipt of complaint/concern within 2 working days of receipt and provide a formal response to Customer within 5 working days of receipt (copied to the Scottish Government for information).

18.3 If the dispute between the Customer and the Service Provider (and/or the Sub-Contractor) cannot be resolved the dispute shall be referred to the Scottish Government, who will independently review the dispute and make a final determination within 10 working days.

18.4 The Service Provider will provide a dedicated feedback e-mail address as part the Induction process. This must be supplemented by a non-digital solution for Customers unable to access email.

18.5 The Induction Pack, issued by the Service Provider to its Customers, must also advise that the feedback be copied to a dedicated Scottish Government inbox. This will allow the Scottish Government to effectively monitor feedback without placing an undue burden on the Service Provider. This feedback will be considered and emerging themes or concerns discussed as a part of contract performance reviews. The Induction Pack needs to be clear that responsibility for dealing with feedback and in particular complaints is initially the responsibility of the Service Provider.

18.6 The Service Provider must ensure that its complaints process includes provision for allegations of serious misconduct.

18.7 The main types of serious misconduct include, but are not limited to:

- racial abuse;
- sexual abuse;
- serious breach of professional conduct;
- theft or fraud; and
- criminal activities.

18.8 The Service Provider must inform the Scottish Government immediately upon receipt of a complaint in this category. The Service Provider must also consider suspending any (employee or) sub-contractor from continuing delivery until any investigations into the complaint has been completed.

18.9 The Service Provider must liaise with the Scottish Government on the outcome of any investigation into a serious complaint. If a serious complaint is upheld, the Service Provider must consider liaising with the relevant professional body and request revocation of approval from the Scottish Government.

18.10 The Service Provider shall report monthly to the Scottish Government on the number and nature of complaints received, source of the complaint, and the average time taken to resolve complaints as detailed within Schedule 1.

19. IT

19.1 The Scottish Government intend to introduce an IT system to support delivery of Fair Start Scotland during the life of the contract. The Scottish Government will work with the Service Provider to develop and introduce a new digitally enabled system developed around the needs of service users.

19.2. In the event that the IT solution is not fully available before Service commencement in April 2018, the Scottish Government will provide a contingency option which may include:

- a hybrid clerical and electronic system.

19.3. The contingency will support referrals to the Service using widely available desktop technologies.

19.4. Scottish Government will provide assistance to the Service Provider in utilising a hybrid clerical and electronic system and will ensure that proper Change Control procedures (see Schedule 3) will be implemented.

19.5. The Service Provider must note that the Scottish Government will not provide an electronic service to manage the Service Provider's relationship with Customers, i.e. a case management solution. The Service provider will undertake their own case management function and put in place their own case management solution.

20. Innovation

20.1 The Scottish Government is committed to a programme of innovation work that will aim to drive greater integration and alignment between employment support and other key services, such as health, justice and skills, during the lifetime of the contract, to improve outcomes for participants and explore how the commissioning of employment services can support this approach.

20.2 Doing so will require an approach on learning and innovation that:

- Encourages, or at the very least does not inhibit, delivery-led innovation by devolved Service Providers;
- Encourages other public services, partners and devolved Service Providers to work together so devolved support services can lead on and participate in new and innovative practices; and
- Creates the space for testing new ideas, taking risks, learning and sharing.

20.3 The Scottish Government is exploring the development of an Innovation Fund alongside the 2018 Service as one way of delivering this approach. The Service Provider may be asked to be involved in the development or delivery of innovation work, subject to further discussion with the Scottish Government.

21. Performance Requirements

21.1 The Scottish Government 2015 consultation document highlighted that any employment programme should pursue sustainable employment as its key outcome and measure of success.

21.2 The Scottish Government has provided clarity on expectations on Customers (both who they are and how many there should be), service requirements and performance expectations, while at the same time leaving scope for Service Providers to draw on their intelligence and experience to secure a robust and ambitious set of contracts which are the foundation for a successful service.

21.3 However, operating an entirely voluntary programme on this scale represents a departure from comparable employment support programmes in the UK over the last 10-20 years, which have been underpinned by degrees of mandatory engagement and systems within which the commissioner has considerable control over both the supply and demand sides of the service.

21.4 Some of these fundamental elements are absent in the devolved Scottish context and this will require a more responsive and partnership focussed relationship between the Scottish Government and the Service Provider to address these challenges collectively.

21.5 Policy development in respect of tackling inequality and Fair Work at Scottish Government level mean that income levels and the need to try to address in-work poverty, aligned to aspirations of a Scottish Living Wage for all – have an increasing importance.

21.6 In addition to the outcome measure set out below, the Service Provider shall measure the extent to which Customers are moving into Scottish Living Wage jobs (and in which sectors) and will work with the Scottish Government to agree how this is gathered.

21.7 For the reasons set out above, the Scottish Government has an aspiration to measure job outcomes through income using the HMRC Real Time Earnings (RTE) data currently available to DWP. Prior to reaching agreement with HMRC, Job Outcomes will be defined as a minimum of 16 hours per week worked at the National Minimum Wage (NMW) or above, appropriate to their age over either a continuous or cumulative period of employment.

21.8 The Service Provider is required to provide evidence to verify the number of hours worked each week by each Customer (and shall obtain a disclaimer from the Customer to allow the Service Provider to contact the employer to verify employment and earnings). As part of the validation process, the Scottish Government will conduct checks on a sample basis to ensure they meet all requirements (see Schedule 2: (Contract Charges, Payments and Pricing)) (and this activity shall also be covered by the disclaimer obtained by the Service Provider).

21.9 For research and evaluation purposes, any available data on actual earnings that can be collected pending agreement with HMRC should be recorded and stored by the Service Provider.

21.10 The performance expectations for Customers are outlined below and represent a minimum level of performance from the Referral Period on each Service Strand and at a Programme level. Details on how the performance expectations have been established are attached at Annex D, (Customer Volumes and Contract Values) of this Schedule.

21.11 Minimum Performance Expectations in respect of the Key Performance Indicators at a Strand Level:

Service Strand	13 week Job Outcomes (% of starts on the Programme)	26 weeks Sustained Job Outcome (% of 13 week Job Outcomes)	52 weeks Sustained Job Outcome (% of 13 week Job Outcomes)
Core Strand	41%	84%	70%
Advanced Strand	27%	84%	70%
Intense Strand	28%	84%	70%

21.12 The above Minimum Performance Expectations are based on the following assumptions of how those starting the Programme will attach to each service strand:

- 14% of Customers will be supported through the Core Service Strand.
- 50% of Customers will be supported through the Advanced Service Strand.
- 36% of Customers will be supported through the Intense Service Strand.

21.13 The Service Provider's performance will be measured on a cohort performance metric. This metric is derived from the following information:

- The number of starts per Service Strand each calendar month;
- The minimum performance level for each Service Strand;
- The profile or distribution for the length of time between Customers being referred to the Service and achieving a job outcome; and
- A one month lag has been added between a job outcome being achieved and a job outcome being claimed to allow for administrative activities.

21.14 Further detail on cohort performance metrics are contained within the operational guidance.

22. Outcomes not eligible as Job Outcomes

22.1 In defining the types of opportunity which may be considered a job outcome and will therefore not count towards the Service Provider meeting the KPIs:

- Community Jobs Scotland training opportunities; and

- any job which has been created through the provision of a wage subsidy. The Scottish Government insist on a drive towards real jobs.

23. Management Information

23.1 In addition to management information gathered from the Scottish Government supporting IT systems, the Service Provider shall provide routine management information reports to the Scottish Government.

23.2 The Service Provider shall provide management information reports or data exchange in electronic and computer readable formats. The format (or online) will use CSV, XML, Word, Excel or other format as appropriate to the purpose of the data. The format, content and transport mechanism of the required management information will be agreed between the Scottish Government and Service Provider. The content and data of the reports will belong to the Scottish Government, and the Scottish Government will define the Data specification standards that the Service Provider will need to comply to.

23.3 Reports are to be provided to the Scottish Government on a monthly basis, no later than 10 working days following the end of each month during the Contract Period. Reports or data extracts may include, but not be limited to, the following information which must be collected and available for reporting as required:

If applicable i.e. Customer does not start on the Service after referral to Service Provider:

- Reason for failure to attend
- Reason for failure to start

Customer information (to be gathered at start of Programme):

- Date of Birth
- Gender*
- Ethnic Group*
- Long-term health condition/ disability*
- Sexual Orientation*
- Religion*
- Gender reassignment*

*Scottish Government will provide advice on the questions to be asked, and the mode of collection to be used

- Name
- Address, including full postcode
- Benefit in receipt of
- NI number
- Contact details and preferred method of contact
- ESOL support needs
- Literacy or Numeracy support needs
- Length of unemployment
- Reason for leaving last job.

*Scottish Government will provide advice on the questions to be asked, and the mode of collection to be used

Referral criteria – whether the Customer is:

- Someone with convictions (someone who has completed a custodial sentence or a community sentence) or offender (someone who is completing a custodial or community sentence)
- Care experienced
- A lone parent
- A refugee
- From an ethnic minority
- A health condition which presents a barrier to employment
- Living in one of the 15% most deprived SIMD areas
- Long term unemployed (2 years+)
- Disabled (as defined in the Equality Act 2010)

On-Programme information

- Programme referrals
- Programme starts
- Job starts:

    - Employer details
    - Contract type
    - Contract hours

- Job Outcome (3 months)
- Job sustainment (6 months)
- Job sustainment (12 months)
- All information relating to and recorded as part of the Customer Action Plan.
- Wider (softer) Customer outcomes -'distance travelled' towards work

Job outcome achieved: (3 months)

- Found permanent employment
- Self employed
- Living/ Scottish Living wage job
- Employment sector

Job sustainment (6 months)

- With same employer as 3 month outcome
- With 1 or more different employers

Job sustainment (12 months)

- With same employer as 3 month outcome
- With same employer as 6 month outcome
- With 1 or more different employers

Other positive destination achieved

- Entered other forms of training
- Progression or return to College
- Progression or return to University

Reasons for leaving Programme without an outcome prior to completion

- Customer does not wish to continue participating (disengages)
- Personal issues prohibiting participation (not health-related)
- Health related issues
- Financial issues

- Relocated / Moved Away
- Serious Injury
- Pregnancy
- Death
- Detained in custody
- Education or training
- Other (please specify)

Provider-based information

- Client/advisor ratios;
- The use of wage subsidies (including Intermediate Labour Market) and their impact on performance;
- Details of any particular areas where there are specific delivery challenges, including but not exclusively rural. Any relevant case studies would be helpful;
- Current levels of co-ordination/integration with other services, how this is used and how well it is working. This will inform priorities for future integration;
- Good news stories;
- Case studies;
- Details of Community Benefits being delivered.

23.4 In addition to the monthly management information report, the Service Provider shall produce an Annual Report in May of each year, and a final overarching Report at the end of the Contract.

23.5 The overarching Annual Report must contain both narrative and statistical data based on aggregated management information up to and including the period of the annual report, along with a broader narrative on the added value and impacts of the Service to both the Service Provider and wider/ local partners.

23.6 The Scottish Government will use the management information to produce statistics, include in published information documents or any such associated requirement to use the information.

24. Performance Management

24.1 The Service Provider shall monitor and report on performance against the Service Levels and the Contract.

24.2 The Key Performance Indicators and Key Delivery Indicators are detailed at Annex E and F of this Schedule. These requirements will be measured as part of the overall performance of the Service Provider, utilising individual Customer case management notes to evidence progress and outcomes.

24.3 The Service Provider's performance against the Service Levels will be checked by the Scottish Government's Performance Management and Operational Support Team on a monthly basis. The Service Provider must provide the Scottish Government with its full cooperation in this process and will be required to provide full access to its systems and evidence as required to conduct the checks at such times as the Scottish government may require.

24.4 The Scottish Government will assess the Service Provider's performance using such means or methods as it considers appropriate in the circumstances (which may include (without limitation) a strategic performance management tool to assess quality, service, delivery and cost).

24.5 The Scottish Government will utilise monthly performance and management information available from the supporting IT or clerical systems, for performance management purposes,

and the Service Provider must provide additional monthly/ ad-hoc management information (as set out in Management Information within paragraph 23 of this Schedule) within 10 Working Days following the end of each month.

24.6 The Scottish Government has the right to request information and access to records in relation to Programme delivery at any time and the Service Provider will provide any and all such information which is requested. Response times for this type of ad-hoc request will be determined by the Scottish Government on a case by case basis at the time of the request, however the Service Provider must note that on occasions, such as receipt of a Request for Information, the Scottish Government's requests will require a prompt response and in any case within such time as the Scottish Government may determine at the time of making the request.

24.7 The Service Provider will be responsible for all costs associated with the provision of management information. Annex E (Performance Expectations) to this Schedule contains the Key Performance Indicators and key delivery Indicators designed to measure delivery, service, quality and cost in relation to the Contract. Any additional Service Levels will be agreed prior to the Commencement Date.

24.8 The Service Provider will be responsible for ensuring delivery of the Services in accordance with the Service Guarantee for the Contract Period.

24.9 Any additional specific Service Levels will be agreed using the procedures set out in Schedule 3 (Change Control Procedures).

24.10 The Service Levels may need to be revised/added to over time and the Service Provider shall continuously improve and reset the Service Levels to increase performance, where appropriate as reasonably requested by the Scottish Government and agreed in accordance with Schedule 3 (Change Control Procedures).

24.11 Duly authorised staff or agents of the Scottish Government shall have the right to visit sites used by the Service Provider to deliver the Service and to be given access to the Service Provider's records and staff (and/or those of its sub-contractor) and to Customers during the hours when the Service Provider is delivering the service with a view to verifying that the Service Provider is delivering the Service in accordance with the Contract.

25. Tracking Period

25.1. Where the Customer leaves the Programme without the Service Provider meeting any of the Outcomes in respect of such Customer, then:

25.1.1. where the Service Provider is able to evidence that the Customer has commenced employment within the 6 weeks immediately following the relevant Customer leaving the Programme (such 6 week period known as the **"Tracking Period"**); and

25.1.2. where such employment started by the relevant Customer during such Tracking period meets the Outcomes

then the Service Provider shall be allowed to claim for the relevant Outcome payments in respect of such Customers.

25.2 Where the Customer leaves the Programme the tracking period lasts for 6 weeks, and will commence on the date a Customer leaves their period of pre-Employment Support without a job.

25.3 This six week period allows the Service Provider to claim Job Outcome payments for Customers who move into employment (that meets the Job outcome definition stated in paragraph 29.11) within six weeks of formally leaving Fair Start Scotland.

26. Monitoring and Evaluation Activities

26.1 The Scottish Government may require additional information from the Service Provider in order to monitor and evaluate the success of provision and their management and delivery of the Services. The Service Provider must co-operate fully with any monitoring and/or evaluation activity commissioned by the Scottish Government. This may include provision of details of Customers' age, gender, ethnicity, disability, progress and achievements.

26.2 Evaluation will seek to investigate the extent to which the Service meets its aims, objectives, Key Performance Indicators, Key Delivery Indicators and process measures. The Service Provider must participate fully in the evaluation and share key learning to help inform the Scottish Government's future service delivery plans. This will include, but not necessarily be limited to, participating in interviews with the Service Provider to learn from their perspectives, assisting in the generation of a sampling frame of Customers from whom interviewees will be selected and providing relevant management information when required. The Service Provider will be required to support the Scottish Government in seeking Customer Consent to use and share data, and to facilitate Customers joining an Experience Panel on attachment to the Programme.

26.3 The Scottish Government is likely to externally commission elements of the evaluation and the Service Provider may be asked to provide information directly to the appointed third parties. The aim of the evaluation is to provide a holistic picture of impacts at an individual, group and system level. For example, elements of the evaluation are likely to include:

i) process measures – to gather feedback from Customers, providers and other stakeholders on factors affecting the delivery of services;

ii) assessment of hard outcomes, using a number of routes where possible, including using Service Providers' management information and through direct surveying of individuals. The Scottish Government is investigating the possibility of linking with data from HMRC on jobs/earnings: and

iii) exploration of softer outcomes - using a mix of methods (e.g. questionnaires, interviews and focus groups) to measure individual and group level impacts such as Customer satisfaction, self-confidence and perceived health benefits.

26.4 The Scottish Government will wish to be able to break findings down to show impacts, for example, for the three Service Strands, at different Lots and for different groups (e.g. age, sex, ethnicity, disability etc.) where possible.

26.5 The management information collected, performance assessment undertaken and annual reports will provide an important contribution to the information needs of the evaluation strategy. The management information requirements are shown at paragraph 23 of this Schedule.

27. Assurance and Fraud Team Reviews

27.1 The Assurance and Fraud Team's primary role is to provide the Scottish Government with an assurance that:

- Payments for employability support services are in accordance with the Scottish Government and Treasury requirements;

- Public funds and Scottish Government data are protected; and

- Value for money has been obtained.

27.2 The Assurance and Fraud Team will review the Service Provider's internal control systems to assess their ability to manage risk across three key areas:

- **Governance Arrangements** – to ensure the Service Provider has robust governance arrangements, systems for tracking and reporting performance and anti-fraud measures;

- **Service Delivery** – to ensure the Service Provider has effective systems for administering the Customer Journey to ensure that Scottish Government is receiving the service it is paying for. The review will also include the management of the supply chain;

- **Financial Procedures** – to ensure the Service Provider has effective systems in place to support their claims for payment, including appropriate segregation of duties.

27.3 The Scottish Government expects the Service Provider to proactively self-assess their management and delivery of the Service. The Assurance and Fraud Team will review the Service Provider's self-assessment activities as part of the assurance process.

27.4 Further about the Assurance and Fraud Team role and the Provider Assurance requirements are detailed in the Terms and Conditions and the Operational Guidance.

28. Continuous Improvement

28.1 The Service Provider will actively seek to improve performance through a policy of Continuous Improvement designed to deliver Service efficiencies, reductions in whole-life costs and improvements in quality and performance throughout the Contract Period.

28.2 The Service Provider's Continuous Improvement Strategy will focus on delivering Service efficiencies and improvements in quality, performance and opportunities for better integration and alignment of services. The Service Provider will maintain a record of Continuous Improvement initiatives and their outcomes.

29. Service Budget and Funding Model

29.1 The Service will be wholly funded by the Scottish Government. The Service will be provided free of charge to all eligible Customers.

29.2 The charges for the Service are detailed within Schedule 2 (Pricing).

29.3 The Scottish Government's 2015 consultation on devolved services highlighted the need for sufficient guaranteed funding to enable smaller organisations to engage and guarantee a level of support for all Customers.

29.4 Therefore the funding model for this Service is intended to reflect the cost of supporting the needs of the Customers in the three Service Strands as outlined in the Customer journeys.

29.5 The Scottish Government will put in place a service fee and payment by results based funding model which is consistent in proportion across all Customer groups.

29.6 The funding model will consist of:

- Implementation Costs;

- Service fee;

- Job outcome fee paid at 13 weeks sustainability; and

- Further Sustained Job Outcome Fees at 26 and 52 weeks of sustained employment.

29.7 The Service Fee is based on 30% of the total contract value (excluding implementation costs) from the Service Providers bid. This will be paid in monthly instalments irrespective of the volumes starting the Programme, as set out in Schedule 2 (Pricing).

29.8 **Job Outcome payments** where a Customer has entered a job and sustained for 13 weeks, 26 weeks and 52 weeks. The proportion of total outcome fees will be set at:

- Job Outcome fee at 13 weeks: 15%
- Sustained Job Outcome fee at 26 weeks: 35%
- Sustained Job Outcome fee at 52 weeks: 50%

29.9 The Service Provider will be able to claim payment for sustained job outcomes following 13, 26 & 52 weeks of employment based on Customer being in work for a cumulative period of 13 weeks in a 16 week period, 26 weeks in a 30 week period and 52 weeks in a 60 week period.

29.10 The Service Provider will be able to claim payment for job outcomes achieved within the 'Profiling and Planning Activities' period (Weeks 1-8) based on the Core Service Strand rate as outlined in Schedule 2 (Pricing).

30. Payment Validation Process

30.1 The Scottish Government will validate outcome payments on a regular basis by conducting a series of pre and post payment checks. Further information about the validation process and the evidence requirements are detailed in Schedule 2, Annex A (Pricing).

31. Key Delivery Indicators - Validation Process

31.1 The Service Provider is required to maintain a robust system of internal control that needs to be sufficient not only to support achievement of Key Delivery Indicators (KDI) but also to allow internal management checks to be undertaken and independent testing and validation, by Scottish Government. The records maintained should document how and when the KDIs were achieved and any appropriate supporting evidence was obtained.

31.2 The Scottish Government does not prescribe the way in which the Service Provider should track Customers or record information about their activity. However, these must be capable.

31.3 The Service Provider remains accountable for making sure that all KDI outcomes are checked.

31.4 KDIs which fail validation or the Scottish Government is unable to validate will be subject to a challenge period. This provides the Service Provider with the opportunity to seek review by submitting additional information which allows the Scottish Government to reconsider.

31.5 Each month the Scottish Government will randomly select for validation a sample of Customer records. Please note, the Scottish Government reserve the right to sample additional records at any point. The Service Provider will be informed by Scottish Government on who has been selected within the sample.

31.6 The sample will be subject to checks to establish if KDIs relevant to the sample have been met.

31.7 Where one or more KDIs have not been met, and following the challenge period, the Service Credit process described at Schedule 2 (Pricing) shall apply.

32. Customer Travel Expenses

32.1 Customers must not be financially disadvantaged due to their attendance at the Service. However, some Customers may **already** receive support for such costs due to a health condition; therefore they must not be over-compensated.

32.2 The Service Provider is responsible for reimbursement of all appropriate travel costs and any additional support costs incurred. The Service Provider must not assume that the Customer is entitled to travel costs, and must ensure appropriate checks are made before payment is made to the Customer, and that the most appropriate mode of transport has been utilised by the Customer depending upon their level of health condition, disability or any other barrier to travel.

32.3 Where the Customers travel costs are to be paid or reimbursed, these costs must not exceed Scottish Government standard travel rates (i.e. those that are currently applicable at the point of costs being incurred by the Customer) which are provided within Schedule 2 (Pricing).

32.4 Data on Customer costs must be provided in accordance with the provision of management information and to meet audit and governance requirements. This will include the submission of receipts and/or vouchers.

33. Childcare Costs

33.1 Customers will be entitled to childcare costs if this is a barrier to attending the Service. The Service must be delivered, where possible, within the hours to suit the Customer, but where this cannot be met, or no alternative funding sources can be identified, childcare costs may be considered.

33.2 The Service Provider is responsible for arranging to provide childcare costs associated with the Customer's attendance on the Service. These will be paid in agreement with Scottish Government at standard rates and reclaimed on an agreed basis.

33.3 Data on Customer costs must be provided in accordance with the provision of management information and to meet audit and governance requirements. This will include the submission of receipts and/or vouchers.

33.4 Further information on agreement of Childcare Costs and the rate of payment will be provided in the Operational Guidance.

34. Additional Costs

34.1 The Service Provider is responsible for payment of any additional costs incurred where a Customer needs extra help to attend and participate fully in the Service. This may include grants, clothing, specialist equipment that is required to support the Customer take up an employment opportunity. Appropriate checks must be made before agreeing to provide the funding requirement, including exploring alternative funding options.

34.2 Data on Customer costs must be provided in accordance with the provision of management information. This will include the submission of receipts or vouchers where appropriate.

34.3 DWP guidance on Access to Work will be updated to reflect devolved employment services. The Service Provider must take note of the guidance in relation to expenses covered by Access to Work and those covered by providers in contracted support for those in work.

35. Open Book Accounting

35.1 Open Book Accounting ("**OBA**") will provide the Scottish Government with information that will be invaluable in helping to understand all costs associated with the Service delivery and help to inform future funding models and Service delivery and design. This includes:

- understanding expenditure (cost base);
- understanding the cost implications of decisions taken or being considered in delivering the Service and forward investment;
- operating and managing the Service to incentivise and drive improvements in cost efficiency;
- how Service Providers and their sub-contractors can work together to develop and implement a proactive approach to Service decision making and create a positive experience for the Customer; and
- help the Scottish Government understand the cost drivers in delivering this service, learn about the prime/sub v consortium delivery approaches and the scope for future efficiencies.

35.2 The Information that the Service Provider will share with the Scottish Government will include, but not be limited to, the following:

- Data on actual Service Provider and sub-contractor costs, margins, trends and volumes. Likely to include both actual and forecast data;
- Information on process, systems and quality controls put in place to manage and ensure compliance;
- Any other financial or non-financial data gathered continuously or periodically that supports innovation, Continuous Improvement or decision making.

35.3 Specific OBA requests from the Scottish Government will be discussed with the Service Provider on a case by case basis.

36. Contract Management and Key Contract Milestones Dates

36.1 The key contracting dates are detailed below. These provide an overview of the Contract timelines, milestones and the final invoicing date which is fully detailed in Schedule 2 (Pricing).

Activity	**Date(s)**
Contract Award	1st Novermber 2017
Implementation and Mobilisation	2nd November 2017 to 31 March 2018
Operational Service Commencement Date (i.e. First Customer Referral)	13 March 2018
Service Delivery Go Live Commencement Date (i.e. Customer Start)	3 April 2018
Last Customer Referral:	2 April 2021
Last Pre-employment Support	1 April 2022
Note: In exceptional cases Pre-employment Support may be extended for up to 6 months for Customers in the Intense Strand. The last date for Customers on Pre-employment Support is:	30 September 2022
Last date for In-work Support (i.e. Contract expiry	24 November 2023

date). Note: This date applies only to Customers assigned to the Intense Service Strand whose pre-employment period was extended by 6 months.	

37. **Contract Extension**

37.1 The Scottish Government, subject to satisfactory Service Provider performance, the continuing need for the service and availability of budget will reserve the option to extend the contract for up to two years as contained in Clause 4.2 of the Contract.

38. Contract Management

38.1 The Scottish Government considers the effective performance and delivery of the Services to be a business critical objective of the Contract. As such, the Service Provider shall be open, flexible and transparent in the operation, management and delivery of the Contract and shall develop and implement appropriate due-diligence, risk management and quality assurance measures to ensure that Services are delivered on time, within budget and in accordance with the Service Levels.

38.2 The Service Provider must provide and maintain adequate management and staff resources, including a Service Manager to support the strategic and day to day operation and management of the contract.

38.3 The Service Manager shall hold a senior position and have sufficient influence with the Service Provider's organisation to be able to promptly respond on the Service Provider's behalf to the Scottish Government's requests, queries and complaints.

38.4 The Service Manager shall act as the single point of contact for the purposes of operating the Contract and will be responsible for the effective mobilisation, implementation, delivery and exit management of the Contract.

38.5 The Service Manager shall ensure that the Service Levels are achieved and consistently high standards of service and best practice are assured and maintained throughout the duration of the Contract.

38.6 The Service Provider must ensure that all staff engaged in the performance of the Contract have and maintain an appropriate level of knowledge and expertise; are appropriately trained and qualified; and are competent to deliver the required Services. This may include, but is not limited to: training on the tasks to be performed; operation of the Contract; and procedures concerning health and safety at work, data protection and sustainability.

38.7 The Service Provider must ensure that there is a sufficient level of trained and competent staff to operate and manage the Contract at all times and that an adequate reserve of trained staff and competent staff are available during holidays, sickness and/or any other absence.

39. Contract Review Meetings

39.1 The Service Manager shall be required to attend monthly Governance and Review meetings with the Scottish Government.

39.2 The Service Manager may also be required to attend additional ad-hoc meetings at times and locations specified by the Scottish Government, including the quarterly meetings referred to in paragraph 13, Partnership, Integration and Alignment.

39.3 The Governance and Review Meetings will address operational issues such as Service delivery and achievement of the Service performance requirements.

39.4 The Scottish Government may on occasion request that specific sub-contractors attend the monthly meetings if this is deemed to be necessary.

39.5 All costs incurred by the Service Provider in attending review meetings will be the responsibility of the Service Provider.

40. Change Control Procedures

40.1 In addition to the service requirements within this Specification, the Service Provider shall embrace changes (proposed by the Scottish Government) to the delivery model to reflect emerging good practice; or adapt to changes to policy to ensure the delivery of the principles and values outlined in this document. Any such requirements will be subject to formal discussions and agreement according to the change control procedures detailed at Schedule 3 (Change Control Procedures).

41. Mobilisation and Implementation

41.1 During the implementation period, the Service Provider shall provide the Services in accordance with the Implementation Plan to ensure the Services will be fully functional in order that: i) the Operational Services will be ready to commence on the Services Commencement Date; and ii) the Go Live Services will be ready to commence on the Services Go-Live Commencement Date.

41.2 The Service Provider will be responsible for managing the successful mobilisation and implementation of the Contract in accordance with the Implementation Plan and shall provide sufficient resources to ensure the availability and provision of the Services in accordance with the Contract from the Service "Commencement Date".

41.3 The Service Provider must submit a detailed Implementation Plan to the Scottish Government for approval no later than 10 Working Days from the **Effective Date (the "Detailed Implementation Plan")**. The Service Provider shall not be entitled to propose any variations to the Scottish Government milestone dates set out in the Initial Implementation Plan.

41.4 The Scottish Government shall review and comment upon the Implementation Plan as soon as reasonably practicable and in any case, no later than 10 Working Days from its receipt. Following such review and consultation, the Scottish Government shall formally approve or reject the Implementation Plan.

41.5 If the Scottish Government rejects the Detailed Implementation Plan, it shall provide its reasons for the rejection and the Service Provider shall have the period of 10 Working Days from the date of the rejection in which to revise and re-submit the Implementation Plan for approval. The parties shall use all reasonable endeavours to resolve any disputes and agree the Detailed Implementation Plan as soon as possible. If the parties are unable to resolve any disputes this shall be referred to the Management Arrangements (Schedule 4).

41.6 The Service Provider will update the Detailed Implementation Plan on a monthly basis (or as otherwise directed by the Scottish Government) until such time as all Milestones have been Achieved and shall submit the updated plan to the Scottish Government's Contract Manager within 10 Working Days prior to the end of each month. The provisions of clauses 40.3 and 40.4 shall apply mutatis mutandis provided that the references to 10 Working days shall be reduced to 5 Working Days.

41.7 The Service Provider will appoint a named Service Manager to manage the mobilisation and implementation of the Contract. The Service Manager will act as the Single Point of Contact (SPoC) for the Scottish Government. The Service Provider will also specify a named contact to the Scottish Government for the escalation and progression of any issues associated with the mobilisation and implementation process.

42. Data Management

42.1 The Service Provider shall ensure that all information held or obtained by the Service Provider in connection with the operation of the Contract is securely and sensitively managed at all times and in accordance with Schedule 9 (Model Contract regarding Data Protection Directive 95/94/EC).

43. Exit Strategy

43.1 The Service Provider shall develop and maintain plans and procedures for the orderly transition of the Services to a successor Service Provider in accordance with Schedule 10 (Exit Management).

44. Business Continuity & Disaster Recovery

44.1 The Service Provider shall have in place and maintain appropriate and relevant Business Continuity and Disaster Recovery plans, policies and procedures in respect of the Services in accordance with Schedule 11 (Business Continuity and Disaster Recovery (BCDR)).

45. Physical Data Security

45.1 The Service Provider shall ensure robust and layered physical security measures are in place at all sites where data is stored. This must include, but not be limited to:

- limited access to server room (authorised personnel only);
- low key appearance;
- limited entry points to server room;
- door control system, including Fire Doors.

Penetration Testing

45.2 The Service Provider must confirm that associated IT systems are tested on an annual basis by an accredited tester and that vulnerabilities are actioned in line with recommended actions.

45.3 The Scottish Government further require that an accredited penetration test specific to the hosted website(s) be conducted annually, or earlier should significant changes be implemented that have the possibility of introducing weaknesses to those systems. Recommended actions should be implemented to remove or mitigate any discovered vulnerabilities. This will ensure that checks are aligned with business objectives (i.e. scope, constraints, deliverables) and that remedial actions are actioned in line with business requirements.

45.4 The Service Provider shall develop and maintain an Information Security Management System and Security Management Plan within the provisions of Schedule 12 (Security).

46. Storage of Data

46.1 The Service Provider must store all data relevant to this Contract (whether personal data or otherwise) in a secure data storage environment which must be located within the European Economic Area.

46.2 This data must be stored in a manner that allows authorised persons to easily access and retrieve data.

47. Risk

47.1 The Service Provider shall, at all times, have in place an appropriate risk management strategy (including a suitable risk management plan and risk logs) for the delivery and support of Services to be provided under the Contract.

47.2 The Service Provider must inform the Scottish Government immediately of any known or foreseeable risks which may have an impact on the operation of the Contract and/or the performance of the Services.

48. Sustainability, Environmental and Community Benefits

48.1 The Service Provider shall comply with the Scottish Government's sustainable development strategy and ethical policy with respect to the delivery of this Contract.

48.2 The Service Provider's policies and processes will support the Scottish Government's 'Greener Scotland' strategic objective including: a proactive approach to sustainable consumption and the efficient use of resources; consideration given to social and environmental consequences; policies which ensure that business activities have a direct positive impact on climate change and energy; and policies which encourage natural resource protection and environmental enhancement.

48.3 The Scottish Government is committed to sustainable procurement and to this end the Service Provider is required to comply with all social and environmental policies in the delivery of Services during the period of the Contract.

48.4 The Service Provider will be required to report to the Scottish Government within their monthly management information reporting, details of any sustainability and environmental measures and achievements.

48.5 'Community Benefits' are social considerations which include not only targeted recruitment & training, but also equal opportunities, training for the existing workforce, supply-chain initiatives, community consultation, 'considerate Supplier' schemes, contributions to education, the promotion of social enterprises and resources for community initiatives.

48.6 The Service Provider shall embrace the Scottish Government's requirement for delivering Community Benefits through the Contract. To assist the Scottish Government in understanding what opportunities exist to deliver benefits to the community through the Contract, the Service Provider shall report to the Scottish Government as part of their monthly management information reporting, details of any Community Benefit measures and achievements such as Targeted Recruitment and Training, skills development, employment, apprenticeships, etc.

48.7 The Public Sector in Scotland is committed to the delivery of high quality public services, and recognises that this is critically dependent on a workforce that is well rewarded, well-motivated, well-led, has access to appropriate opportunities for training and skills development, are diverse and is engaged in decision making. These factors are also important for workforce recruitment and retention, and thus continuity of service. Public Bodies in Scotland are adopting Fair Work practices, which include:

- a fair and equal pay policy that includes a commitment to supporting the Living Wage, including, for example being a Living Wage Accredited Employer;

- clear managerial responsibility to nurture talent and help individuals fulfil their potential, including for example, a strong commitment to Modern Apprenticeships and the development of Scotland's young workforce;

- promoting equality of opportunity and developing a workforce which reflects the population of Scotland in terms of characteristics such as age, gender, religion or belief, race, sexual orientation and disability;

- support for learning and development;

- stability of employment and hours of work, and avoiding exploitative employment practices, including for example no inappropriate use of zero hours contracts;

- flexible working (including for example practices such as flexi-time and career breaks) and support for family friendly working and wider work life balance; and

- support progressive workforce engagement, for example Trade Union recognition and representation where possible, otherwise alternative arrangements to give staff an effective voice.

48.8 In order to ensure the highest standards of service quality in this Contract, the Service Provider shall take a similarly positive approach to Fair Work practices as part of a fair and equitable employment and reward package.

Annexes to the Specification and Service Levels

Annex A to Schedule 1: Sources of Information

1. Creating a Fairer Scotland: A New Future for Employability Support in Scotland: http://www.gov.scot/Resource/0049/00498123.pdf

2. Creating a Fairer Scotland: Employability Support: http://www.gov.scot/Resource/0048/00481121.pdf

3. ONS, Labour Force Survey, Apr-Jun datasets, 2016 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/workingandworklesshouseholds/aprtojune2016

4. The Scottish Government Disability Delivery Plan http://www.gov.scot/Publications/2016/12/3778

5. ONS Labour Force Survey, June-August 2016 https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/bulletins/uklabourmarket/october2016

6. Equalities Act 2010 http://www.legislation.gov.uk/ukpga/2010/15/introduction

7. *Scottish Index of Multiple Deprivation (SIMD)*[7] http://www.gov.scot/Topics/Statistics/SIMD

8. Employability Pipeline http://www.employabilityinscotland.com/employability-pipeline/

9. EU How to Guides on Supported Employment http://www.euse.org/index.php/resources/how-to-guides

10. The Scottish Living Wage http://scottishlivingwage.org/

11. Supported Employment Framework for Scotland http://www.gov.scot/Resource/Doc/303629/0095168.pdf

12. The Scottish Government http://www.gov.scot/Home

13. The Scottish Business Pledge https://scottishbusinesspledge.scot/

14. The Scottish Government's Diversity and Equality Policy http://www.gov.scot/Topics/People/Equality

15. The Scottish Government's Labour Market Strategy (including Fair Work Agenda) http://www.gov.scot/Publications/2016/08/2505

Annex B to Schedule 1: Service Guarantee

All Customers will be entitled to a service guarantee, as summarised below:

Initial Engagement (Day 1)

- Initial contact within 5 working days of referral to arrange first interview.
- A face to face initial assessment within 10 working days of referral to confirm eligibility and an action plan for the Discovery and Planning phase (see below) of the Programme.
- Allocation to a named key worker who will be your adviser for the duration of the Programme
- Agreement of a Participation Agreement, setting out the commitments of each party.
- **Intense Service Strand Only:** Speedy referral to specialist providers for Customers assessed as needing support through the Intense Service Strand.

Discovery and Planning Phase (1 to 8 weeks)

- Weekly interventions with key worker
- Face to face monthly review with key worker;
- Baseline assessment of employability skills;
- Better Off in Work calculation and financial planning; and
- Planning for additional support to be provided by external or partner services;

- **Core and Advanced Service Strands Only:** Development of a detailed personalised Employment Action Plan which sets out agreed activities and timescales to help you into work including activities for overcoming barriers including engagement with external services, current skills, employment history, vocational training needs, employment aspirations, monitoring and review arrangements and in-work support plan.

- **Intense Service Strand Only:** Vocational Profiling leading to an individual action plan

Pre Work Support (9 to 52 weeks)

- Minimum of 3 hours weekly contact with key worker;
- 1 to 1 coaching by key worker as necessary;
- Face to face formal monthly review with key worker;
- Quarterly distance travelled assessment and feedback;
- Employability activities as detailed in the individual Employment Action Plan;
- Engagement with external or partner services as detailed in the individual Employment Action Plan;
- Monthly workplace reviews (if on work placement);
- Weekly job search activities;
- Employer engagement including support for interviews and negotiations of reasonable adjustments; and
- Financial guidance.

- **Intense Service Strand Only:** Support to overcome recruitment barriers;
- **Intense Service Strand Only:** Job matching with suitable vacancies, including job carving; and
- **Intense Service Strand Only:** Job carving during work experience placements (if necessary)

In-Work support (Job entry date + 52 weeks)

- An In-Work Support Action Plan, detailing timeline for workplace reviews with employer, future training and career development goals and actions;
- Minimum of weekly contact with key worker, fading as appropriate;
- Minimum monthly workplace review with employer, reducing over time as appropriate
- Workplace induction; Support at workplace training (if necessary);
- Support to develop workplace relationships;
- Financial guidance; Advice for employer, training for employer's staff (as necessary); and
- Individual exit planning in the final stages of the Programme

- **Intense Service Strand Only:** Job Analysis;
- **Intense Service Strand Only:** Task Analysis (if necessary); and
- **Intense Service Strand Only:** Workplace job coaching, reducing over time as appropriate

Annex C to Schedule 1: Lots

Lot	Local Authorities Areas	% share of potential Customers *
Glasgow	Glasgow	**20.0%**
Lanarkshire	North Lanarkshire South Lanarkshire	**13.2%**
Tayside	Angus Dundee City Perth and Kinross	**7.6%**
Forth Valley	Clackmannanshire Falkirk Stirling	**5.2%**
East	City of Edinburgh East Lothian Fife Midlothian Scottish Borders West Lothian	**22.2%**
Southwest	East Ayrshire Dumfries and Galloway North Ayrshire South Ayrshire	**10.5%**
North East	Aberdeen City Aberdeenshire	**5.9%**
Highlands and Islands	Argyll and Bute Eilean Siar Highland Moray Orkney Islands Shetland Islands	**6.4%**
West	East Renfrewshire Inverclyde Renfrewshire East Dunbartonshire West Dunbartonshire	**9.0%**

* References to Lot 'West' in this Specification are for information purposes only. Lot West if for Supported Businesses.

Annex D to Schedule 1: Customer Volumes & Contract Values

Assumption on the number of individuals attaching to each service strand

Until the Scottish Government Segmentation Tool has been finalised and tested, the Scottish Government has built assumptions, at a national level, on the extent to which each of our Customer groups will be supported within the Core, Advanced and Intense Service Strands. These assumptions were provided to inform Service Providers in developing their proposals for the each Lot(s).

Service level	Eligible Groups	Take Up	Total	% of Starters
Core	JSA 24+			**14%**
	Early Entry			
	Total Eligible Population		12,700	
	Initial Take Up	*60%*	7,620	
	Final Take Up	*70%*	**5,334**	
Advanced	JSA 24+			**50%**
	ESA WRAG			
	Early Entry			
	Total Eligible Population		45,100	
	Initial Take Up	*60%*	27,060	
	Final Take Up	*70%*	**18,942**	
Intense	ESA WRAG			**36%**
	Early Entry			
	Total Eligible Population		18,390	
	Initial Take Up	*60%*	11,034	
	Final Take Up	*70%*	7,724	
	ESA Support		1,500	
	Non-Claimants		4,500	
	Total		**13,724**	
	Total Attachments		**38,000**	

The above percentages have been used by the Scottish Government to determine the minimum performance expectations detailed in this Annex.

Recognising the entirely voluntary nature of the Programme, the Scottish Government has built in assumptions on how the eligible population relates to programmes starts based on available comparable evidence of both voluntary and mandatory programmes in Scotland and the UK:

- The Scottish Government has assumed an initial take up rate of 60% in each service strand which articulates the extent to which we expect the eligible population to volunteer and be referred to the Programme, this is described as the initial take up rate;

- The Scottish Government has also assumed that 70% of those voluntary referrals will actually start on the Programme, this is described as the final take up rate.

The above assumptions have been used by the Scottish Government to determine the minimum volume/performance expectations detailed in this Annex. In addition, the Scottish Government has included a drop-out rate of 10% against all Service Levels, again reflecting the entirely voluntary nature of the Programme, on those who start the Programme.

Calculation of the Minimum Performance Expectation

The Scottish Government has established Minimum Performance Expectations (MPE) at the 13 week Job Outcome point on each service level. Analysis was conducted to determine which client groups are most likely to be supported in each service level and a performance baseline for each strand was created by assessing the performance of comparable client groups over the duration of the Work Programme in Scotland.

The Scottish Government then tested this Work Programme baseline against key differences in the 2018 Scottish service, including its voluntary nature, to identify performance uplift within the 2018 programme. When added to the Work Programme baseline, this creates the MPE for the service.

Service Level	Scottish Government Client Groups	Work Programme Groups	WP Performance	SG Performance Uplift	Minimum Performance Expectation
Core	JSA 24+ Early Entry	JSA 25 and over JSA Early Entrants	30%	11%	41%
Advanced	JSA 24+ ESA WRAG Early Entry	JSA 25 and over New ESA claimants: Excluding 12 Month prognosis claimants JSA Prison Leavers	17%	10%	27%
Intensive	ESA WRAG ESA Support Early Entry Non-Claimants	New ESA claimants: Excluding 12 Month prognosis claimants New ESA claimants: 12 Month prognosis claimants only JSA Prison Leavers ESA Ex-Incapacity Benefit	14%	14%	28%

Sustainment of performance at the 26 and 52 weeks points is consistent across all service levels and is based on comparable data on UK and Scottish Contracted Employment Support programmes.

LOT split based on contract value and the minimum volume expectations

The table below sets out the Lots shares based on the percentage benefit claimant share and minimum programme starts (38,000).

The data has been calculated by assessing the total population of JSA, ESA and UC benefit claimants in Scotland and calculating each Lot's percentage share of this total.

Lots	Glasgow	Lanarkshire	Tayside	Forth Valley	East	Southwest	Northeast	Highlands and Islands
Local Authorities	Glasgow	North Lanarkshire South Lanarkshire	Angus Dundee City Perth and Kinross	Clackmannanshire Falkirk Stirling	City of Edinburgh East Lothian Fife Midlothian Scottish Borders West Lothian	Dumfries & Galloway East Ayrshire North Ayrshire South Ayrshire	Aberdeen City Aberdeenshire	Argyll and Bute Eilean Siar Highlands Moray Orkney Islands Shetland Islands
% Benefit Claimant Share	20%	13.2%	7.6%	5.2%	22.2%	10.5%	5.9%	6.4%
Estimated Contract Value (£)	19,100,000	12,600,000	7,300,000	5,000,000	21,300,000	10,100,000	5,600,000	6,200,000
Estimated Starts	7,600	5,000	2,900	2,000	8,400	4,100	2,200	2,400

Note. The table above excludes information for Lot: 'West' which is reserved for Supported Businesses.

LOT Split on Minimum Performance Expectations

Lot: Highlands and Islands								
Strand	**Assumed Starts %**	**Assumed Starts**	**13 Week Job Outcome %**	**13 Week Job Outcome**	**26 Week Sustain % of 13 Week JO**	**26 week Sustain**	**52 week sustain % of 13 week JO**	**52 week sustain**
Core	14%	336	41%	138	84%	116	70%	96
Advanced	50%	1200	27%	324	84%	272	70%	227
Intense	36%	864	28%	242	84%	203	70%	169
Total	**Total**	**2400**	**29%**	**704**	**84%**	**591**	**70%**	**493**

Annex E to Schedule 1: Key Performance Indicators

Ref.	Key Performance Indicator	Measurement
1.	**Job Outcomes:** Must be for a minimum of 16 hours per week paid at NMW which has lasted 13 weeks in a 16 week period. For self-employment the Customer must have traded independently, working at least 16 hours per week for their business for 13 weeks at NMW; provided the job meets the outcome criteria you will be entitled to claim for a job outcome. This will be confirmed by the individual.	The Service Provider's performance in respect of this Outcome shall be reviewed and measured monthly by the Scottish Government using performance data to ensure the Service Provider's monthly projections on performance have been achieved. Paragraphs 21.13, 21.14 and 25 if this Schedule shall apply
2.	**Sustained Job Outcomes (26 weeks)':** Must be for a minimum of 16 hours per week paid at NMW. Employment must have lasted 26 weeks out of 30 weeks. For self-employment the Customer must trade independently working at least 16 hours per week for their business for 26 weeks at NMW, from date of employment outcome. This will be confirmed by the individual. (Breaks in employment must total no more than 4 weeks).	The Service Provider's performance in respect of this Outcome shall be reviewed and measured monthly by the Scottish Government using performance data to ensure the Service Provider's monthly projections on performance have been achieved. Paragraphs 21.13, 21.14 and 25 if this Schedule shall apply
3	**Sustained Job Outcomes (52 weeks):** Must be for a minimum of 16 hours per week paid at NMW. Employment must have lasted 52 weeks out of 60 weeks. For self-employment the Customer must have traded independently, working at least 16 hours per week for 52 weeks out of 60 week period at NMW, from date of employment. This will be confirmed by the individual. (Breaks in employment must total no more than 8 weeks).	The Service Provider's performance in respect of this Outcome shall be reviewed and measured monthly by the Scottish Government using performance data to ensure the Service Provider's monthly projections on performance have been achieved. Paragraphs 21.13, 21.14 and 25 if this Schedule shall apply
	*Note: Any period of self-employment can only be counted once regardless of whether the participant has one or multiple self-employed occupations during that period.	

Annex F to Schedule 1: Key Delivery Indicators

All Strands

Ref.	Key Delivery Indicators	Measurement	Service Level
1	**Start Date and Service Induction (Stages 4 and 5)**. Start/Induction Interview to be completed face to face within 5 Working Days from receipt of the referral.	Measured monthly via a random Sample of Service Providers' caseload management records	90%
2	**Start Date and Service Induction (Stages 4 and 5)**. For any Customer whose Start/Induction interview is not completed within the 5 Working Days timeline as outlined in Ref.1 above, the Start/Induction Interview must be completed within 10 Working Day from receipt of the referral.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
3	**Start Date and Service Induction (Stages 4 and 5)**. Service Provider must immediately notify the Customer and Referral Agency in writing of the date and time of their Start Date/Induction Interview after the warm handover process detailed in Stage 3.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
4	**Start Date and Service Induction (Stages 4 and 5)**. 48 hours prior to the Start Date/Induction Interview a courtesy telephone call to be made by the Service Provider to the Customer to alleviate any Customer's concerns.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
5	**Start Date and Service Induction (Stages 4 and 5)**. At the Induction Interview, the Service Provider must provide each Customer with an Induction Pack.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
6	**Intervention / Customer Engagement (All Stages)** At every weekly face to face intervention, a Customer's personalised Action Plan will be reviewed and updated to reflect progress and agreement of future activities and actions.	Measured monthly via a random Sample of Service Providers' caseload management records	100%

Ref.	Key Delivery Indicators	Measurement	Service Level
7	**Intervention / Customer Engagement (All Stages)** Face to face formal monthly review between the Key Worker and the Customer to take place.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
8	**Segmentation Tool** Segmentation Tool must be completed by Customer prior to start on the Programme.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
9	**Segmentation Tool** Service strand to be confirmed by end of week 3 commencing from the referral of the relevant Customer.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
10	**In Work Support Plan (Stage 10)** A detailed In Work Support (IWS) Plan to be agreed with the Customer within 10 Working Days of job start.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
11	**Procedure for Disengagement by Customer** The Service Provider must contact the Customer within 1 Working Day to establish circumstances surrounding disengagement from being notified by the Customer that they will not continue with the Programme.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
12	**Procedure for Disengagement by Customer** If the Service Provider is unable to engage the Customer within 5 Working Days of either i) failing to attend service provision they must contact the Referral Agency or ii) failing to establish circumstances surrounding disengagement as outlined in 11 above.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
13	**Customer Programme Exit and Leaver Plan (Stages 8 and 9)**. The Service Provider must produce a detailed Leavers Plan for each Customer returning to the Referral Agency, within 10 Working Days of Customer's end date.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
14	**Complaints**. The Service Provider must acknowledge receipt of complaints/concerns within 2 Working Days of receipt.	Measured monthly by the Scottish Government via a random sample of Service Providers' caseload management records.	100%

Ref.	Key Delivery Indicators	Measurement	Service Level
15	**Complaints**. Service Provider must provide a formal response to Customer within 5 Working Days (copied to the Scottish Government) of the complaint being raised.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
16	**Specialist Support** Service Provider must facilitate immediate referrals and access to specialist support to address health problems, including professional help to manage mental/physical health conditions and well-being interventions.	Measured monthly via a random Sample of Service Providers' caseload management records	100%

Annex F to Schedule 1: Key Delivery Indicators - Intense Strand Only

Ref.	Key Delivery Indicator	Measurement	Service Level
17	**In Work Support Plan (Stage 10)** Job Analysis must be undertaken for each Customer entering employment to inform the In-Work Support Action Plan, which, with Customer consent, must be agreed with the employer.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
18	**Vocational Profiling** All Customers must be offered Vocational Profiling.	Measured monthly via a random Sample of Service Providers' caseload management records	100%
19	**Supported Employment Model and Individual Placement and Support** The Supported Employment Model for disabled people and Individual Placement and Support (IPS) must be available and offered.	Measured monthly via a random Sample of Service Providers' caseload management records	100%

Key Delivery Indicators: Performance Reporting

Ref.	Delivery Indicator	Measurement	Service Level
20	**Management Information** The Service Provider is required to provide management information to the Scottish Government in accordance with this Specification	Accurate monthly management information must be provided within 10 Working Days of the end of each month.	100%
21	**Stakeholder Engagement Plan** The Service Provider is required to provide an updated Stakeholder Engagement Plan every 3 months commencing from the **"Commencement Date"** and report progress of partnership, integration and alignment activities with local organisations and services.	Measurements and milestones to be agreed post contract award.	100%

Annex G to Schedule 1: Integration and Alignment with Other Scottish Government Services

The Scottish Government has set out a programme of public sector reform which includes an ambition for much greater integration of services. A list of current Scottish Government funded Services is set out below, with an indication of its purpose and how it will align or integrate with the new employment programme.

There must be no expectation that these initiatives will run for the duration of Fair Start Scotland contract.

Service	**Integration and Alignment**
Opportunities for All – an offer of training or education for young people not in education employment or training.	The new service is part of the integrated offer of support.
Activity Agreements	The new service will be part of the support young people on Activity Agreements will be able to access from age 18 if it is appropriate for them.
Community Jobs Scotland	Service Providers may believe this service suitable and appropriate for their Customers, in which case and on the assumption that eligibility conditions are met and a suitable opportunity is available, they can do so. However, this will not be considered a job outcome for the purposes of the contract pricing model.
SERI	SERI is a wage subsidy for new jobs including apprenticeships. Service Providers may believe this suitable and appropriate for their Customers, in which case and on the assumption that eligibility conditions are met and a suitable opportunity is available, they can do so. However, this will not be considered a job outcome for the purposes of the contract pricing model.
Open Doors In Work Support 16-29	This is specialist in-work support. The Scottish Government expect high quality in-work support as part of the new service. Access to this for service Customers would be duplication of funded support, so will not be possible.
Modern Apprenticeships	Articulation from employment services to Modern Apprenticeships is a key ambition. Access to Modern Apprenticeships will be defined as a job outcome. The apprenticeship must be expected to last 12 months or more.
Employability Fund	The Employability Fund will remain a key part of the pre-contracted support provision for DWP Customers and will align with devolved services at this time. Service Providers must make provision for short sharp skills interventions available to Customers in line with Customer need and opportunities in the local labour market.
Individual Learning Accounts	Participants on the new service cannot access ILAs.

Annex H to Schedule 1: Additional information on Supported Businesses

The Scottish Government is committed to furthering the development of supported businesses in Scotland. We have set up the Supported Business Advisory Group (SBAG), the Framework for Supported Factories and Businesses; actively promoting the use of Regulation 21 of the Public Contracts (Scotland) 2015 Regulations within public sector procurement and commissioning the 2013 independent Review of Supported Businesses in Scotland. SBAG is chaired by the Minister for Business, Innovation and Energy.

One of the aims of SBAG is to increase the amount of public contracts placed with Supported Businesses. Scottish Government is represented on SBAG and is expected to be an exemplar by increasing the amount of contracting activity with Supported Businesses by considering sustainability as part of the award criteria for regulated procurements and where possible the use of Regulation 21 of the Public Contracts (Scotland) 2015 Regulations.

A Supported Business is defined in the Public Contracts (Scotland) Regulations 2015 as:

> "an economic operator whose **main aim is the social and professional integration of disabled or disadvantaged persons** and **where at least 30% of the employees of the economic operator are disabled or disadvantaged persons**;"

Annex I to Schedule 1: Technical Response Document

Technical Response is provided under separate word document

Annex J to Schedule 1: Clarifications

Clarifications are provided under separated word document

This and the following 11 pages comprise Schedule 2 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 2 - PRICING SCHEDULE

1. The Purchaser will pay the Service Provider the Contract Charges as outlined in Annex 2 to this Schedule for the provision of the Services in accordance with the Specification and Service Levels (Schedule 1) and the rest of the Contract.

2. All Outcome payments shall be FIXED (i.e. not subject to change) in respect of Customer referrals received during the Initial Referral Period as outlined in clause 4.1.1 of the Contract (Period) and any increase to the Outcome payments following the Initial Renewal Period shall be determined solely in accordance with paragraph 3 of this Schedule.

2.1 All Service fees shall be fixed (i.e. not subject to change) for the period commencing from the Services Commencement Date until the end of the Initial Referral Period and any increase to the Service fees following the Initial Referral Period shall be determined solely in accordance with paragraph 3 of this Schedule.

3. Indexation

3.1. Should the option to extend the Contract be taken up, at the sole discretion of the Purchaser, based upon clause 4.2 of the Contract (Period), the Contract Charges for such extended period shall be negotiated between the Parties and such negotiated price shall not exceed the Contract Charges derived using the following methodology:

3.2. Indexation will be applied to the Outcome payments in accordance with the annualised Consumer Price Index ("CPI"), as provided by the Office for National Statistics, for the December in the Purchaser's financial year immediately preceding the commencement date of the relevant Contract extension. Any such increase shall be applied once per extension on the commencement date of the relevant Contract extension and the indexed rates will be applicable over the entire duration of the relevant extension. For example, the Outcome payments for 2021-22 would be uplifted by 2.5% if annualised CPI for December 2020 was 2.5%. These indexed fixed fees would be applicable over the 1 year extension period.

3.3 Indexation will be applied to one year's Service fees (being the total Service fees as shown in Annex 2 to this Schedule divided by four (4)) in accordance with the annualised Consumer Price Index ("CPI"), as provided by the Office for National Statistics, for the December in the Purchaser's financial year immediately preceding the commencement date of the relevant Contract extension. Any such increase shall be applied once per extension on the commencement date of the relevant Contract extension and the indexed rates will be applicable over the entire duration of the relevant extension. For example, the Service fees for 2021-22 would be uplifted by 2.5% if annualised CPI for December 2020 was 2.5%. These indexed fixed fees would be applicable over the 1 year extension period.

4. Not Used

5. Supporting Information related to Pricing

The funding approach has the following payment elements and ratios:

5.1. Implementation Costs

5.1.1 The Purchaser recognises that some costs will be incurred prior to the Services Commencement Date. Implementation costs can be paid as a part of the Contract if the Service

Provider considers this beneficial. Where Implementation costs are paid, these shall be outlined in Annex 2 to this Schedule.

5.1.2. Where the Service Provider wishes to be paid for these costs separately they will be fixed and on a cost recovery basis only. These costs be paid in arrears at such times as outlined in Annex 2 to this Schedule and subject to the retention outlined in paragraph 5.2.3 of this Schedule and always after they have been incurred by the Service Provider. No mark up or Service Provider profit margin in relation to these costs will be accepted. Additionally, only those costs which need to be met by the Service Provider prior to the Services Commencement Date will be considered for payment by the Purchaser. For example, where the cost relates to staff salaries, only payments incurred by the Service Provider in respect of any period in which they are employed on the implementation of the Programme as outlined in the Contract up to the Services Commencement Date will be considered for payment.

5.1.3. Where the Implementation costs are paid under the Contract, the Purchaser shall withhold 30% of the total Implementation costs until the Service Provider commences to provide all the Go Live Services. The Purchaser shall release the retained Implementation costs where the Service Provider is ready to provide the Go Live Services even where no Customers have been referred to the Service Provider, provided that this is not due to a Default of the Service Provider.

5.2. Service Fee

5.2.1. The service fee will equate to 30% of the total Contract price (excluding any implementation and contingency costs agreed). The service fee is intended to provide a degree of certainty in meeting fixed costs associated with delivery of the Service and will be paid monthly in arrears. The service fee shall be payable over three years from the Services Commencement Date in respect of the period from the Services Commencement Date until the end of the Initial Referral Period.

5.2.2. The service fee will then be further divided into Year 1; Year 2; and Year 3 Service Fees based on 50% (Year 1); 30% (Year 2); and 20% (Year 3) of the initial 30% of the total Contract price. These amounts will then be further divided into equal monthly payments for each year.

Example:

(Note: the overall cost is not intended to represent actual costs)

Overall Costs for Service (excluding Implementation)	£ 100,000
Total Service Fee	£ 30,000 (£ 100,000 x 30%)
Year 1 Service Fee	£ 15,000 (£ 30,000 x 50%)
Monthly Service Fee	£ 1,250 (£ 15,000 / 12 months
Year 2 Service Fee	£ 9,000 (£ 30,000 x 30%)
Monthly Service Fee	£ 750 (£ 9,000 / 12 months)
Year 3 Service Fee	£ 6,000 (£ 30,000 x 20%)
Monthly Service Fee	£ 500 (£ 6,000 / 12 months)

5.3. Outcome Payments

5.3.1. The overall amount available for Outcome payments will equate to 70% of the total Contract price (excluding any implementation and contingency costs agreed).

5.3.2 The Service Provider shall render an invoice on a monthly basis in respect of all the Outcomes achieved during the previous month in respect of Customers. The Service Provider shall provide to the Purchaser any and all evidence the Purchaser may request to support such invoice.

5.4. Achievement of Job Outcomes

5.4.1. Job Outcomes payments will be made on a unit price basis, which will be calculated by dividing 15% of the Outcome payments described above by the number of Job Outcomes as outlined in Annex 2 to this Schedule. These payments will only be made in respect of Customers to whom Key Performance Indicator 1 applies, as outlined in Annex E to the Specification.

5.5. Achievement of First Sustainment Payments

5.5.1. First Sustainment payments will be made on a unit price basis, which will be calculated by dividing 35% of the Outcome payments described above by the number of first sustainment Outcomes as outlined in Annex 2 to this Schedule . These payments will only be made in respect of Customers to whom Key Performance Indicator 2 applies, as outlined in Annex E to the Specification.

5.6. Achievement of Second Sustainment Payments

5.6.1. Second Sustainment Payments will be made on a unit price basis, which will be calculated by dividing 50% of the Outcome payments described above by the number of second sustainment Outcomes as outlined in Annex 2 to this Schedule . These payments will only be made in respect of Customers to whom Key Performance Indicator 3 applies, as outlined in Annex E to the Specification.

5.7 Contingency Costs

As detailed in Section 19 of the Specification, the IT solution for managing referrals and outcome payments is still under development. The Service Provider's contingency costs for a hybrid clerical and electronic system are outlined in Annex 2 to this Schedule.

5.8 Payment validation

The provisions of Annex 1 to this Schedule 2 shall apply to all payments by the Purchaser to the Service Provider. No payment in respect of paragraph 5.4 shall be due unless the Service Provider's claim for payment has been validated in accordance with the procedures outlined in that Annex 1 to this Schedule.

6. Service Credits

6.1. The Service Credits shall be calculated with reference to any of the below events occurring for an individual Customer who engages with the Programme. For the avoidance of doubt this includes pre start employability activities through to their end of In-Work Support activities. The number of events which have occurred shall be multiplied with the Service Credit value allocated to each event.

6.2. The Service Credit value shall be calculated using the Service Provider's service fee as set out below:

- The service fee for each service strand shall be divided by the number of Customers anticipated in each strand as outlined in Annex D of Schedule 1 to calculate a notional service fee per Customer per strand ("Notional Service Fee").

6.3. The Service Credit value in respect of Key Delivery Indicators 1-16, as detailed within Annex F to Schedule 1, shall be equivalent to one sixteenth of the Notional Service Fee for each occasion where the Service Provider fails to meet the specified service level for the relevant Key Delivery Indicator.

6.4. For the Intense Strand only, the Key Delivery Indicators 17-19 the Service Credit value shall be equivalent to the entire Notional Service Fee for that strand for each occasion where the Service Provider fails to meet the specified Service Level for the relevant Key Delivery Indicator.

Service Credits	Service Credit Value
Failure to meet Key Delivery Indicators 1-16	£ per Key Delivery Indicator failure
Failure to meet Key Delivery Indicators 17-19	£ per Key Delivery Indicator failure

6.5. Where relevant, following identification of an event occurring, the Purchaser shall render an invoice in respect of the amount to be recovered as detailed in the methodology for calculation of Service Credits outlined in this Schedule. Such invoice shall be payable by the Service Provider to the Purchase no later than 30 days from the date of invoice.

Annex 1 to Schedule 2

Payment Validation Process

1.1. The Service Provider must have robust financial and accounting procedures in place to meet audit requirements. These must include details of all financial transactions and supporting evidence in relation to all payments. The Service Provider shall provide assistance to the Purchaser for the Purchaser to be able to complete the validation process as the Purchaser may require.

1.2. The Service Provider shall only submit accurate claims for payments that they are entitled to under the Contract. The Purchaser will utilise its own systems to satisfy itself that the claims are valid. This will include a series of checks to confirm that Customers have started and remained in employment or self-employment for the required period of time and have worked the hours and fulfil any other requirements as outlined in the Contract.

1.3. The Service Provider is required to maintain a robust system of internal control that not only supports any claims for payment but also allows internal management checks to be undertaken and independent testing and validation, by the Purchaser and other external bodies. The records maintained shall document how and when the appropriate supporting evidence was obtained.

1.4. Where a Customer has not given consent to contact employers, this must be recorded by the Service Provider. In these cases the Purchaser will only contact the Customer. Where consent has been given, the Purchaser will contact the relevant employer and/or the Customer in an attempt to validate the claim.

1.5. The Service Provider shall track Customers and record information about their employment activity. There is however specific information in relation to each Customer that the Service Provider is required to document and submit to the Purchaser when it submits claims for payment in respect of an Outcome:

- Whether the period is employment or self-employment
- Employer/s contact details including address, contact name, full business telephone number and email address
- The Customer's contact details
- Start date of employment/self-employment
- End date of employment/self-employment (if applicable)
- The number of hours worked in each week
- Confirmation that the Customer is earning National Minimum Wage (NMW) as a minimum
- The working/shift pattern

1.6. The Service Provider remains accountable for making sure that all Outcomes are checked prior to making a claim for payment and that all such claims must be valid at the point of submission for payment.

1.7. The Service Provider shall promptly notify the Purchaser where it becomes aware of any information in respect of claims for payment and/or payments (prior to sampling in accordance with paragraphs 1.9 and 1.20) which require a claim to be withdrawn to allow the Purchaser to arrange for the recovery of funding where the fee has been paid and to allow the claim to be removed from the system.

1.8. Claims which fail validation or which the Purchaser is unable to validate will be subject to a challenge period. This provides the Service Provider with the opportunity to seek review by submitting additional information which allows the Purchaser to have another attempt at validation.

1.9. Each month the Purchaser will randomly select for validation a sample of claims which have been paid by the Purchaser (the size of the sample to be determined by the Purchaser) in

the previous month. If the total of claims paid is less than the specified sample in any month then all claims will be selected. The Purchaser reserves the right to sample additional claims at any point in its sole discretion. The Service Provider will be informed by the Purchaser of the Customers who have been selected within the sample.

1.10. The sample of Job Outcome claims will be subject to checks to establish if Customers have been in work, for at least 16 hours per week, for 13 weeks out of 16 weeks (from the job start date), paid at NMW with no breaks in employment (or, in the case of a self-employed Customer, they have traded independently for at least 13 weeks) as outlined more specifically in the KPIs.

1.11. The Purchaser may in the future decide to measure Outcomes through income using the HMRC Real Time Earnings (RTE) data currently available to DWP.

1.12. The Service Provider can meet the KPI even if the Customer's employment is made up of more than one employer as long as 16 or more hours are completed and paid at NMW in each week. Where the Purchaser identifies that the other conditions for the KPI have not been met in respect of the Customer's employment or self-employment, then the claim will fail validation.

1.13. Where the Purchaser identifies during validation that the job start date is prior to the date the Customer started on the Programme, the claim will fail validation, unless the Customer has increased hours to a minimum of 16 hours per week paid at the NMW, as outlined more specifically in the Key Performance Indicators in Annex E to the Specification.

1.14. Where the Purchaser establishes that a Customer has not been in work for a sufficient time at the point when the claim is submitted to the Purchaser to meet the requirement but at the point of validation the Customer meets all requirements as outlined in the relevant Key Performance Indicators, the claim will be treated as a Technical Pass.

1.15. Where a Customer has not given consent to contact employers the Purchaser will only attempt validation via the Customer. Where the employer is unable/ unwilling to validate the claim, the Purchaser will contact the Customer. In cases where the Purchaser is experiencing difficulty making contact with the employer and/or the Customer, the Purchaser may, but is not obliged to, contact the Service Provider to confirm the details the Service Provider has supplied. For example, where the Purchaser believes that the Service Provider has submitted incorrect or incomplete information (e.g. unobtainable telephone numbers).

1.16. The Service Provider is required to establish the correct information and supply it promptly to the Purchaser to maximise the chances of positive contact. If the Service Provider does not provide the detail that enables the Purchaser to complete validation, the claim will fail validation.

1.17. Error rates are derived from checking a representative sample of claims and extrapolating against the remaining population of claims. This means the correct level of payment and performance will be attributed to a Service Provider. Therefore the Purchaser will not accept a request to withdraw a claim once a sample has been drawn.

1.18. There are four possible validation results:

- **"Pass"** – An employer and/or Customer confirms the condition for payment has been met, as set out in the Outcome

- **"Technical Pass"** – at the manual validation stage there are two scenarios:

    - An employer/Customer confirms that there is a valid claim however the details provided by the employer and/or Customer and the details supplied by the Service Provider differ. The Purchaser will inform the Service Provider of the correct information and the Service Provider will update its records. The payment will not be recovered and will not contribute to the error rate for extrapolation.

- If the Purchaser establishes that a Customer has not been in work for a sufficient time within the claim period to meet the requirement but at the point of validation they have (and meet all requirements), the claim will be treated as a Technical Pass. The payment will not be recovered and will not contribute to the error rate for extrapolation.

- **"Fail"** – An employer/Customer provides information which means the condition for payment, as set out in the KPIs, has not been met. The claim is recorded as an error and will contribute to the error rate for extrapolation.

- **"Unable to Validate"** – the Purchaser has either not been able to contact the employer and/or Customer, or the employer and/or Customer are unable/ unwilling to provide the information required to validate the claim.

1.19. Unable to Validate claims will be apportioned across the other validation results. Before any of these claims are apportioned, the Service Provider will have the opportunity to seek review by submitting additional information that will allow the Purchaser to have another attempt at validation. Where the claim is not validated as a result of such review or the Service Provider does not request a review, this will contribute to the error rate for extrapolation.

Sustained Job Outcome Validation

1.20. Each month the Purchaser will randomly select for validation a sample (the size of the sample to be determined by the Purchaser) of claims which have been paid by the Purchaser to the Service Provider , that have been paid in the previous month for validation in respect of the second and the third KPIs. If the total of claims paid is less than the specified sample in any month then all will be selected. The Purchaser reserves the right to sample additional claims at any point in its absolute discretion. The Service Provider will be informed by the Purchaser of the Customers who have been selected within the sample.

1.21. The sample for Sustained Job Outcomes (26 weeks) will be subject to checks to establish if Customers have been in work for a minimum of 16 hours per week paid at NMW which has lasted 26 weeks out of 30 weeks. Breaks in employment must total no more than 4 weeks during the 30 week period as outlined in the second KPI.

1.22. The sample for Sustained Job Outcomes (52 weeks) will be subject to checks to establish if Customers have been in work for a minimum of 16 hours per week paid at NMW which has lasted 52 out of 60 weeks. Breaks in employment must total no more than 8 weeks during the 60 week period as outlined in the third KPI.

1.23. Where the Purchaser establishes that a Customer has not been in work for sufficient time when the claim is submitted to the Purchaser to meet the requirement but at the point of validation they have (and meet all requirements), the claim will be treated as a Technical Pass.

1.24. Where consent to contact the employer has been given but the employer is unable/unwilling to validate the claim, the Purchaser will contact the Customer. In cases where the Purchaser is experiencing difficulty making contact with the employer and/or the Customer, the Purchaser may, but is not obliged to, contact the Service Provider to confirm the details it has supplied. For example, where the Purchaser believes that the Service Provider has submitted incorrect or incomplete information (e.g. unobtainable telephone numbers). The Service Provider is required to establish the correct information and supply it promptly to the Purchaser to maximise the chances of positive contact during the validation window. If the Service Provider does not provide the detail that enables the Purchaser to validate the claim, the claim will fail validation.

1.25. Error rates are derived from checking a representative sample of claims and extrapolating against the remaining population of claims. This means the correct level of payment and performance will be attributed to a Service Provider. Therefore, the Purchaser will not accept a request to withdraw a claim once a sample has been drawn.

1.26. There are four possible validation results:

• Pass – An employer/Customer confirms the condition for payment, as set out in the Sustained Job Outcome definition outlined in the Key Performance Indicators, has been met.

• Technical Pass – at the manual validation stage there are two scenarios:

- An employer/Customer confirms that there is a valid claim however the details provided by the employer and/or Customer differ from the details the Service Provider has supplied. The Purchaser will inform the Service Provider of the correct information and the Service Provider will update its records. The payment will not be recovered and will not contribute to the error rate for extrapolation.

- If the Purchaser establishes that a Customer has not been in work for a sufficient time within the claim period to meet the requirement but at the point of validation they have (and meet all other requirements), the claim will be treated as a Technical Pass. The payment will not be recovered and will not contribute to the error rate for extrapolation.

• Fail – An employer and/or Customer provides information which means the condition for payment, as set out in the Sustained Job Outcome definition, has not been met. The claim is recorded as an error and will contribute to the error rate for extrapolation.

• Unable to Validate – the Purchaser has either not been able to contact the employer/ Customer, or the employer and/or Customer are unable/ unwilling to provide the information required to validate the claim.

1.27. Unable to Validate claims will be apportioned across the other validation results. Before any of these claims are apportioned, the Service Provider will have the opportunity to seek review by submitting additional information that will allow the Purchaser to have another attempt at validation. Where the claim is not validated as a result of such review or the Service Provider does not request a review, this will contribute to the error rate for extrapolation.

1.28. Not Used

Payment Validation Review Process (Outcomes and Sustained Job Outcomes)

1.29. Following the completion of the payment validation exercise, the Service Provider will receive a report from the Purchaser detailing the claims that have either failed and/or which the Purchaser has been Unable to Validate. This report will also give the information that informed the validation decision. Before any of these claims are used to calculate the error rate for extrapolation, the Service Provider will have 10 Working Days to consider this information and to submit additional information to the Purchaser. All requests for review, together with any supporting information or evidence, must be received within 10 Working Days of the validation failure report being provided to the Service Provider. Late requests will not be accepted and will be returned.

1.30. The Service Provider must ensure that requests for review are proportionate and reasonable and that additional information is provided to that supplied in the original claim that was not available at the time of the original submission. If the Purchaser is of the view that the additional information supplied allows the Purchaser to go back to an employer or Customer, another attempt to validate the outcome will be made by the Purchaser.

1.31. Where the original validation result failed because the Purchaser had been given information from an employer or Customer and/or employer that positively invalidates a claim, this is a fail and the Purchaser shall not attempt to revalidate the claim with the Customer.

1.32. Where the Service Provider has provided additional information that will allow the Purchaser to make additional enquires in the attempt to obtain a positive validation result, the Service Provider is shall email the Purchaser detailing all such relevant and appropriate information. The Service Provider may also provide physical evidence, however this will only be used in an attempt to revalidate the appropriate outcome, and will not be accepted in its own right. The Service Provider is shall submit any documentation to the Purchaser in line with Scottish Government security guidelines.

1.33. All requests for review, together with any supporting information or evidence, must be received within 10 Working Days of the validation failure report being sent to the Service Provider. Late requests will not be accepted and will be returned to the Service Provider. If no formal request has been received by the Purchaser by close of business on the 10th Working Day following the sending of such validation failure report, then cases which the Purchaser has been Unable to Validate or which have failed will be apportioned and an extrapolation report and invoice (if applicable) will be raised by the Purchaser. Such invoice shall be payable by the Service Provider to the Purchaser no later than 30 days from the date of the invoice.

1.34. Once the cases have been reviewed, the Purchaser will present the review findings to a review board. This board will have senior representation from the Purchaser. The purpose of the review board is twofold; to be satisfied that any reviewed decisions will stand up to scrutiny to the Purchaser's Internal Audit and Audit Scotland and to approve the original validation decision, if it remains unchanged. The review board may also request that the Purchaser or the Service Provider supply further information or investigation before finalising decisions.

1.35. Following approval from the review board, the Purchaser will notify the Service Provider of the results and issue the Service Provider with an extrapolation report. These decisions will have gone through a rigorous challenge process signed-off by senior representatives of the Purchaser to ensure that all valid claims are recognised. Decisions are final and no further challenge will be accepted.

1.36. Following a challenge, an unable to validate claim could be overturned to a Pass or a Fail. If it becomes a Fail, any such fails will contribute to the error rate for extrapolation.

1.37. The Purchaser operates regular review boards and extrapolation will be applied following the outcome of the review board.

Extrapolation Process Job Outcomes and Sustained Job Outcomes

1.38. The following paragraphs detail the extrapolation process. This process will be applied separately to payments made in respect of the first KPI and the second and third KPIs.

1.39. Following the review board decisions at the end of the relevant validation period, the number of Passes, Fails, Unable To Validates and Technical Passes, will be totalled for each monthly sample in the period. Claims that are positively invalidated contribute to the error rate for extrapolation.

1.40. A number of claims assessed to be Unable to Validate will be apportioned as fails. The number is calculated as follows:

a = number of Unable to Validate Outcomes
b = number of Outcome Fails
c = number of Outcome Technical Passes
d = number of Outcome Passes
e = denominator = b + c + d
f = total number of Outcome Payments in the sample = a + b + c + d
g = simple fail rate = b/f
h = Apportioned Unable to Validate Outcomes = a*b/e
(rounded to the nearest whole number),
I Total Outcome Fails = b+ h
Apportioned fail rate = i/f

1.41. The process for validation and extrapolation will be fully outlined within the Operational Guidance.

1.42 Where relevant, following such review, the Purchaser shall render an invoice in respect of the amount to be recovered as detailed in the extrapolation report as outlined in this Schedule. Such invoice shall be payable by the Service Provider to the Purchaser no later than 30 days from the date of the invoice.

Annex 2 – pricing breakdown

Implementation Costs – Not Applicable

Service Fees							
	Total Available Service Fee £	Year 1 Total Service Fee (50% of Total Available Service Fee for the service level £	Year 1 Monthly Service Fee £	Year 2 Total Service Fee (30% of Total Available Service Fee for the service level £	Year 2 Monthly Service Fee £	Year 3 Total Service Fee (20% of Total Available Service Fee for the service level) £	Year 3 Monthly Service Fee £
Core	[redacted]						
Advanced							
Intense							

Outcome Fees				
	Total available for outcomes (70% of Input Sheet Main Total for the service level) £	Total Amount for Job Outcomes (15% of Total Available £	Total Amount for 1st Sustainment Payments (35% of total Available) £	Total Amount for 2nd Sustainment Payments (50% of total Available) £
Core	[redacted]			
Advanced				
Intense				

Outcome Fees – Unit Cost			
	13 Week JO Payment £	26 Week Sustainment Payment £	52 week Sustainment payment £
Core	[redacted]		
Advanced			
Intense			

Contingency Costs (refer to para 5.7 of Schedule 2)	
Costs based on clerical activity being the contingency	[redacted]

- **Note:** *Contingency Costs abased upon 0.32 FTE for the full 4.25 years of the contract* [redacted] *(pa)), plus* [redacted] *of JMS development costs.*

This and the following 2 pages comprise Schedule 3 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 3 – CHANGE CONTROL PROCEDURES

1. CHANGE CONTROL PROCEDURES

1. General

1.1 Any change to the Contract shall be subject to the Change Control Procedures as set out below. For these purposes, a "**Change**" means any proposed amendment or change (including any proposed additional or substituted Schedules or Annexes), or any proposed change to the Services and/or the Contract.

1.2 The Purchaser may at any time request, and the Service Provider may at any time recommend a Change only in accordance with the Change Control Procedure as set out in this Schedule.

1.3 Neither Party shall unreasonably withhold its agreement to any Change. In the event that the Service Provider withholds its agreement to a Change, the Purchaser may, at its discretion perform the applicable Change itself where practicable at the Purchaser's cost.

1.4 Until such time as a Change is made in accordance with the Change Control Procedure, the Service Provider shall, unless otherwise agreed in writing by the authorised representatives of both Parties, continue to supply the Services as if the request or recommendation had not been made.

1.5 Any discussions which may take place between the Purchaser and the Service Provider in connection with a request or recommendation before the authorisation of a resultant Change shall be without prejudice to the rights of either Party.

1.7 Any work undertaken by the Service Provider or its subcontractor(s) which has not been agreed in accordance with the provisions of this Schedule shall be undertaken entirely at the expense and liability of the Service Provider.

1.8 For the avoidance of doubt, any Change which is necessary to ensure that the Services and any Deliverables meet the Specification and Service Levels (detailed at Schedule 1) shall be performed at no cost to the Purchaser.

2. Change Procedures

2.1 The Service Provider must have an appropriate structure and process in place to manage future developments, training, administration tasks and change requests from the Purchaser.

2.2 The Service Provider must acknowledge change requests received from the Purchaser within 2 Working Days. The Service Provider must be able to provide this in electronic and paper format. The Service Provider can follow up with the Purchaser if additional clarification is required regarding the Changes (s) and/or Service(s) requested.

2.3 Where either Party so requests, the Parties shall discuss a Change. Such discussion concerning a Change shall take place between the Purchaser and the Service Provider no later than ten (10) Working Days from either Party's request to discuss a Change unless the Parties agree otherwise. The discussion shall result in any one of the following:

(a) no further action being taken;
(b) a request to change the requirements of a Customer or the Services

2.4 Where a written request for an amendment (as outlined in the Request for Change Form included in this Schedule) is received from the Purchaser, the Service Provider shall, unless otherwise agreed, submit a CCN to the Purchaser within ten (10) Working Days of the date of the request which embodies substantially the terms of the request.

2.5 A recommendation to amend by the Service Provider shall be submitted as a CCN directly to the Purchaser at the time of such recommendation.

2.6 Each CCN shall contain:

(a) the title of the Change;
(b) the originator and date of the request or recommendation for the Change;
(c) the reason for the Change;
(d) full details of the Change including any amendments to the Contract including the Specification and the Pricing Schedule;
(e) the price, if any, of the Change and the Service Provider's methodology in arriving to such price (if relevant)
(f) effort in man days to implement the Change;
(g) a timetable for implementation together with any proposals for acceptance of the Change;
(h) a schedule of payments, if appropriate;
(i) details of the likely impact, if any, of the Change on other aspects of the Services to be provided including but not limited to:

i. the personnel to be provided;
ii. the payment profile;
iii. working arrangements;
iv. other contractual issues;

2.7 For each CCN submitted, the Purchaser shall, within the period of the validity of the CCN:

(a) allocate a sequential number to the CCN;
(b) evaluate the CCN and, where appropriate, request further information in relation to the Change and/or the CCN which further information shall be provided promptly by the Service Provider;
(c) approve the CCN;
(d) notify the Service Provider of the rejection of the CCN.

2.8 A CCN signed by both the Service Provider and the Purchaser shall subsequently constitute an amendment to the Contract. Work should not commence prior to both Parties' signature and any work carried out prior to such signature shall be at the Service Provider's cost.

2.9 Any potential Changes to either systems or processes will be presented to the Purchaser's Contract Manager (as may from time to time be appointed by the Purchaser) for approval to proceed.

3 Charges

3.1 The charges which apply to the Change will be as outlined in the CCN which has been approved by both Parties in accordance with paragraph 2.8. It is for the Service Provider to propose the applicable charges when producing the CCN in accordance with paragraph 2.6. The Parties (each acting reasonably) will discuss and endeavour to agree the charges for the Change which is being proposed.

This and the following 4 pages comprise Schedule 4 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 4 – MANAGEMENT ARRANGEMENTS

Governance

1. Contract Manager

1.1. The Purchaser's Contract Manager will be the main point of contact for the Service Provider.

1.2. The Purchaser's Contract Manager will manage the performance of the Service Provider including, but not limited to, the following:

- reviewing the overall management, operation and delivery of the Service Provider
- appraising the Service Provider against its KPIs and KDIs
- setting the strategic direction of the Service Provider's activities
- developing and implementing agreed marketing and communication approaches monitoring the cost-effectiveness of the operation of the Service Provider to ensure value for money
- responding to escalated key issues raised by the Service Provider or by the Purchaser in relation to the operation of and delivery under the contract, including, for example relating to performance, budget and other issues that are likely to have an impact upon the Purchaser's priorities and objectives.
- ensuring effective collaboration and links between the Purchaser and the Service Provider
- agreeing changes to the operation of the Service Provider

1.3. The Purchaser's Contract Manager will also receive the various performance reports as detailed below and as required in terms of the Contract. The Contract Manager may request relevant information from the Service Provider, as the need arises, and act as a key contract contact point for questions, proposals or requests from the Service Provider.

1.4. The Service Provider's Contract Manager will be the main point of contact for the Purchaser Contract Manager in relation to the Service Provider's performance of the Services. The Service Provide Contract Manager shall be responsible for liaising with the Purchaser Contract Manager in relation to all of the matters listed in paragraph 1.2 above (and shall provide all assistance and information requested by the Purchaser Contract Manager in relation to this. In addition, the Service Provider Contract Manager shall be responsible for supporting the strategic and day to day operation and management of the contract.

1.5 The Service Provider shall not change the Service Provider Contract Manager without Approval,

1.6 Office facilities for the Service Provider will not be provided by the Purchaser.

2. Reporting Arrangements

2.1 The Service Provider will report to the Purchaser on a range of aspects in relation to its performance under the Contract as outlined in paragraph 23 (Management Information) of Schedule 1 (Specification and Service Levels) on a regular basis as part of it meeting its requirements under the appointment.

3. Contract Review Meetings

3.1. In addition to the Contract Review Meetings as detailed in paragraph 39 (Contract Review Meetings) of Schedule 1 (Specification and Service Levels), during the first **three** months from the Effective Date (or longer as the Purchaser may consider necessary), there may be a requirement for ad-hoc meetings between the Purchaser's and the Service Provider's core team to discuss progress and identify any performance issues. All relevant current and pipeline projects will be discussed at these meetings, with a focus on those where there are issues to report and other relevant matters arising from time to time.

3.2. Written dashboards, or similar, outlining activity and progress against each Milestone will be provided by the Service Provider to the Purchaser in reasonable time priorto each meeting for consideration by the Purchaser's Contract Manager, and in any event not less than three Working Days prior to the meeting. This will form the basis for identifying any performance and/or compliance issues at an early stage.

3.3. Issues and risks will be discussed, and actions agreed and minuted by the Service Provider (such minutes to be provided to the Purchaser's Contract Manager for approval as agreed as soon as possible after the meeting or in any event no later than three Working Days prior to the next scheduled meeting).

4. Information Management / Performance Reporting

4.1 The format and content of the required management information will ultimately be agreed between the Purchaser and Service Provider, however in part the requested information as identified within paragraph 23 (Management Information) of Schedule 1 (Specification and Service Levels) may also include the following:

- Total value of sub-contracted spend in relation to the delivery of the Contract.
- Number of sub-contractors delivering goods or services in relation to the Contract.
- Confirmation that sub-contractor are paid within 30 days in accordance with the terms and conditions of the Contract. Reasons for any failure to comply.
- Number of SMEs delivering goods or services in relation to the Contract.
- Value of SME spend in relation to the Contract.
- Details of Health and Safety incidents relating to delivery of the Contract.

4.2 Reports are to be provided to the Purchaser on a (calendar) monthly basis, no later than 10 Working Days following the end of each month during the Contract Period.

4.3 All documents shall be submitted in electronic format and compatible with the Purchaser systems to enable access to and use of such documents by the Purchaser's Contract Manager as necessary.

4.4 Where the Service Provider fails to present a progress report or the final monitoring report and fails to furnish an acceptable written explanation of the reasons why it is unable to comply with this obligation, the Purchaser shall raise the issue via paragraph 6 below.

5. NOT USED

6. Dispute Resolution

6.1 The Parties shall attempt to resolve any dispute between them arising out of, or in connection with, this Contract within 20 Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute as follows.

6.2 Any dispute will, in the first instance, be presented to the Service Provider's Contract Manager and the Purchaser Contract Manager for resolution.

6.3 If the Service Provider's Contract Manager and the Purchaser Contract Manager cannot agree on a resolution, then a separate meeting will be held between the senior management of the Service Provider and the Purchaser for resolution.

6.4 If the dispute cannot be resolved by the Parties pursuant to this paragraph, the Parties shall refer it to mediation pursuant to the procedure set out at paragraph 6A to this Schedule unless:

a) the Purchaser considers that the dispute is not suitable for resolution by mediation;

or

b) the Service Provider does not agree to mediation.

6.5 The obligations of the Parties under this Contract shall not be suspended, cease or be delayed by the reference of a dispute to mediation and the Service Provider shall comply fully with the requirements of this Contract at all times.

6A. **Mediation**

6A.1 For the purposes of this mediation, the following terms are defined as follows:

"**CEDR**" means the Centre for Effective Dispute Resolution of International Dispute Resolution Centre, 70 Fleet Street, London EC4Y 1EU (www.cedr.com);

and

"**Contract Mediator**" means a neutral adviser or mediator chosen by agreement between the Parties.

6A.2. A Contract Mediator shall be appointed or, if the Parties are unable to agree upon a Contract Mediator within 10 Working Days after a request by one Party to the other or if the Contract Mediator agreed upon is unable or unwilling to act, either Party shall within 10 Working Days from the date of the proposal to appoint a Contract Mediator or within 10 Working Days of notice to either Party that he is unable or unwilling to act, apply to the CEDR to appoint a Contract Mediator.

6A.3. The Parties shall within 10 Working Days of the appointment of the Contract Mediator meet with him in order to agree a programme for the exchange of all relevant information and the structure to be adopted for negotiations to be held. If considered appropriate, the Parties may at any stage seek assistance from the CEDR to provide guidance on a suitable procedure.

6A.4. If the Parties reach agreement on the resolution of the dispute, the agreement shall be reduced to writing and shall be binding on the Parties once it is signed by their duly authorised representatives.

6A.5. Failing agreement, either of the Parties may invite the Contract Mediator to provide a non-binding but informative opinion in writing. Such an opinion shall be provided on a without prejudice basis and shall not be used in evidence in any proceedings relating to this Contract without the prior written consent of both Parties.

6A.6. If the Parties fail to reach agreement in the structured negotiations within 60 Working Days of the Contract Mediator being appointed, or such longer period as may be agreed by the Parties, then, for the purposes of clause 54.2 (Dispute Resolution), the dispute cannot be resolved in accordance with the Management Arrangements.

7. Continuous Service Improvement

7.1 Both Parties acknowledge the need for continuous improvement over the Contract Period as outlined in paragraph 28 (Continuous Improvement) of Schedule 1 (Specification and Service Levels) and that the Purchaser have paid the Service Provider for resources that are expected to deliver service improvement.

7.2 The Service Provider will deliver continuous improvement in the Services provided under this Contract, throughout the Contract Period.

7.3 The Service Provider recognises continuous improvement by following the 6 key principles of Scottish Government which are integral to creating a fairer Scotland (as defined within Annex A to Schedule 1).

7.4 Continuous improvement will be monitored by the Purchaser as part of the process for Service Provider management and review.

7.5 The Service Provider must put in place appropriate policies, processes, tools, methodologies and/or resources to continuously improve the service throughout the Contract Period and provide improved value for money.

7.6 During the Contract Period, the Service Provider shall be required to make proposals to the Purchaser which will:

a) improve the Service(s);

b) improve technology or methodology used in connection with the Services;

c) deliver Service efficiencies, reductions in whole-life costs and improvements in quality and performance.

7.7 The Service Provider must put in place a process to capture, assess, report and make recommendations to the Purchaser on initiatives and proposals for continuous improvement in the provision of the Services.

8. Complaints: Definition

8.1 Any communication from a Customer which meets any of the following criteria shall be classed as a complaint:

8.1.1 any communication identified by the Customer as a complaint;

8.1.2 any query or concern about the quality and/or performance of the Services received by the Customer;

8.1.3 any query or concern about any communications, or failure to communicate, through telephone, electronic means, letter or face to face, including the behaviour of anyone, involved in the delivery of the Services

("**Complaint**").

8.2 Where a Customer raises more than one Complaint relating to different areas of service or delivery, these shall be treated as separate Complaints.

9. Complaints: Handling

9.1 The Service Provider shall put in place a system for handling Complaints, which shall be defined and monitored centrally, be transparent, be easily accessible and be well publicised, as detailed in paragraph 18 (Feedback, Suggestions, Complaints and Escalation) of Schedule 1 (Specification and Service Levels).

10. Complaints: Resolution

10.1 The Service Provider shall adhere to the Complaints resolution process as outlined within paragraph 18 (Feedback, Suggestions, Complaints and Escalation) of Schedule 1 (Specification and Service Levels).

11. Complaints: Reporting

11.1 The Service Provider shall report monthly to the Purchaser on the number and nature of Complaints received, source of the Complaint, and the average time taken to resolve Complaints as detailed within paragraph 18 (Feedback, Suggestions, Complaints and Escalation) of Schedule 1 (Specification and Service Levels).

This and the following single page comprise Schedule 5 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 5 – KEY INDIVIDUALS

1. Operations Director – [redacted]
2. Service Manager – T.B.A
3. Integration Manager – T.B.A

Details to be provided by Service Provider following Contract Award.

This and the following single page comprise Schedule 6 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 6 – APPROVED SUB-CONTRACTORS

approved Sub-Service Provider(s)	Relevant obligations
1. Life Skills	Core, Advance and Intense Service Strand Highlands (Dingwall, Invergordan, Inverness), Moray, Orkney Islands, Shetland Islands)
2. Momentum	Intense Strand (Highlands–Dingwall, Invergordan, Inverness)
3. 2020 Clearview	Core and Advance Strand (Highlands – Wick)
4. Argyll and Bute Council	Core, Advance and Intense Service Strand (Argyll and Bute)
5. Lochaber Hope	Core, Advance and Intense Service Strand (Highlands – Fort William, Portree)
6. Third Sector Hebrides	Core, Advance and Intense Service Strand Eilean Siar

This and the following single page comprise Schedule 7 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 7 – SERVICE PROVIDER SENSITIVE INFORMATION

Type of information specified as Service Provider Sensitive Information	**Reason why information is sensitive**	**Duration of sensitivity**
1.1.3 Customer Journey - Stages	To release details of the names of our customer journey - stages would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.4 Customer Journey - Services Strand	To release details of the names of our customer journey – services strand would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.5 Proposed Delivery Mechanism	To release details of the names of our proposed delivery mechanism would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.6 Appendix 1 - Supply Chain Split Remove contact names.	To release details of the names of our contacts in the supply chain would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.7 Part 6 of ITT - Subcontractor Declarations Remove contact names.	To release details of the names of our contacts in the supply chain would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.9 Delivery Locations Remove contact names and locations.	To release details of the names of our contacts and their delivery locations would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.10 Appendix 2 - Subcontractor Locations and Facilities Remove contact names and locations.	To release details of the names of our contacts names and locations would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.12 Stakeholder Engagement Remove contact names.	To release details of the names of our contacts would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.

Type of information specified as Service Provider Sensitive Information	Reason why information is sensitive	Duration of sensitivity
1.1.13 Appendix 3 - Stakeholder Engagement Plan Remove contact names.	To release details of the names of our contacts would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.1.15 Employer Engagement Remove contact names.	To release details of the names of our contacts would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.2.1 Management Structure	To release details of our management structure would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.2.2 Staffing Resources / Proposals to Ensure Robust Delivery	To release details of our staff resources would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.2.3 Resource Plans	To release details of our staff resources would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.3.1 Performance Offer	To release details of the names of our performance offer would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
1.5.2 Performance Management	To release details of the names of our performance management processes would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
Commercial Envelope – Tender price	To release details of our tender price would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.
Commercial Envelope – Commercial Questionnaire	To release details of the names of our commercial questionnaire would be detrimental to our commercial interests exempt under Paragraph 43 (2) of the FOI Act.	We expect this information to remain commercially sensitive for the next 3 years.

This and the following single page comprises Schedule 8 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 8 – PARENT COMPANY GUARANTEE

NOT USED

This and the following 13 pages comprise Schedule 9 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 9 – MODEL CONTRACT REGARDING DATA PROTECTION DIRECTIVE 95/46/EC

Model Contract

STANDARD FORM CONTRACT TO ASSIST COMPLIANCE WITH OBLIGATIONS IMPOSED BY
ARTICLE 17 OF THE DATA PROTECTION DIRECTIVE 95/46/EC

(FOR USE BY DATA CONTROLLERS AND DATA PROCESSORS LOCATED WITHIN THE EUROPEAN ECONOMIC AREA WHERE THE PARTIES HAVE ENTERED INTO A SEPARATE DATA PROCESSING AGREEMENT)

THIS AGREEMENT is made on……and ……20[ ].

BETWEEN:

(1) THE SCOTTISH MINISTERS (the "Controller"); and

(2) PeoplePlus Group Limited (incorporated in, or existing and established under the laws of, United Kingdom (Company registered number 05722765) whose registered office is at 19-20 The Triangle, Ng2 Business Park, Nottingham, NG2 1AE (the "Processor").

BACKGROUND

(A) The Controller processes Personal Data in connection with its business activities;

(B) The Processor processes Personal Data on behalf of other businesses and organisations;

(C) The Controller wishes to engage the services of the Processor to process personal data on its behalf in relation to **Fair Start Scotland**;

(D) Article 17(2) of the Data Protection Directive 95/46/EC (as hereinafter defined) provides that, where processing of personal data is carried out by a processor on behalf of a data controller the controller must choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures;

(E) Articles 17(3) and 17(4) of the Data Protection Directive require that where processing is carried out by a processor on behalf of a controller such processing shall be governed by a contract or legal act binding the processor to the controller stipulating, in particular, that the processor shall act only on instructions from the controller and shall comply with the technical and organisational measures required under the appropriate national law to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure or access and against all other unlawful forms of processing;

(F) In compliance with the above-mentioned provisions of Article 17 of the Data Protection Directive the
Controller and Processor wish to enter into this processing security Agreement.

THE PARTIES HEREBY MUTUALLY AGREE AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 In this Agreement the following words and phrases shall have the following meanings, unless inconsistent with the context or as otherwise specified:

"**Data Protection Directive**" shall mean Directive 95/46/EC of the European Parliament and Council of 24th October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

"**national law**" shall mean the law of the Member State in which the Processor is established;

"**personal data**" shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic cultural or social identity;

"**processing of personal data**" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alternation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

"**sub-contract**" and "**sub-contracting**" shall mean the process by which either party arranges for a third party to carry out its obligations under this Agreement and "Sub Contractor" shall mean the party to whom the obligations are subcontracted; and

"**Technical and organisational security measures**" shall mean measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorised disclosure oraccess and against all other unlawful forms of processing.

2. CONSIDERATION

2.1 In consideration of the Controller engaging the services of the processor to process personal data on its behalf the Processor shall comply with the security, confidentiality and other obligations imposed on it under this Agreement.

3. SECURITY OBLIGATIONS OF THE PROCESSOR

3.1 The Processor shall only carry out those actions in respect of the personal data processed on behalf of the Controller as are expressly authorised by the Controller.

3.2 The Processor shall take such Technical and Organisational Security Measures as are required under its own national law to protect personal data processed by the Processor on behalf of the Controller against unlawful forms of processing. Such Technical and Organisational measures shall include, as a minimum standard of protection, compliance with the legal and practical security requirements set out in Appendix 1 of this Agreement.

4. CONFIDENTIALITY

4.1 The Processor agrees that it shall maintain the personal data processed by the Processor on behalf of the Controller in confidence. In particular, the Processor agrees that, save with the prior written consent of the Controller, it shall not disclose any personal data supplied to the Processor by, for, or on behalf of, the Controller to any third party.

4.2 The Processor shall not make any use of any personal data supplied to it by the Controller otherwise than in connection with the provision of services to the Controller.

4.3 The obligations in clauses 4.1 and 4.2 above shall continue for a period of five years after the cessation of the provision of services by the Processor to the Controller.

4.4 Nothing in this agreement shall prevent either party from complying with any legal obligation imposed by a regulator or court. Both parties shall however, where possible, discuss together the appropriate response to any request from a regulator or court for disclosure of information.

5. SUB-CONTRACTING

5.1 The Processor shall not sub-contract any of its rights or obligations under this Agreement without the prior written consent of the Controller.

5.2 Where the Processor, with the consent of the Controller, sub-contracts its obligations under this agreement it shall do so only by way of a written agreement with the Sub-Contractor which imposes the same obligations in relation to the security of the processing on the Sub-Contractor as are imposed on the Processor under this Agreement.

5.3 For the avoidance of doubt, where the Sub-Contractor fails to fulfil its obligations under any sub-processing agreement, the Processor shall remain fully liable to the Controller for the fulfilment of its obligations under this Agreement

6. TERM AND TERMINATION

6.1 This Agreement shall continue in full force and effect for so long as the Processor is processing personal data on behalf of the Controller.

6.2 Within [insert the number of days agreed by the parties] days following termination of this Agreement the Processor shall, at the direction of the Controller, (a) comply with any other agreement made between the parties concerning the return or destruction of data, or (b) return all personal data passed to the Processor by the Controller for processing, or (c) on receipt of instructions from the Controller, destroy all such data unless prohibited from doing so by any applicable law.

7. GOVERNING LAW

7.1 This Agreement shall be governed by and construed in accordance with the national law of the Member state in which the Controller is established.

AS WITNESS this Agreement has been signed on behalf of each of the parties by its duly authorised representative on the day and year first above written.

SIGNED on behalf of [CONTROLLER]

(Authorised signatory)

(Print name and title)

SIGNED on behalf of [PROCESSOR]

(Authorised signatory)

(Print name and title)

APPENDIX 11

1. Legal requirements

1.1 The Processor shall, in respect of the processing of personal data on behalf of the Controller, identify and comply with any specific security provisions imposed by its national law.

2. Practical security measures

2.1 In compliance with its obligations under clause 3.2 with regard to the processing of personal data on behalf of the Controller, the Processor, as a minimum requirement, shall give due consideration to the following types of security measures:

2.1.1 Information Security Management Systems;

2.1.2 Physical Security;

2.1.3 Access Control;

2.1.4 Security and Privacy Enhancing Technologies;

2.1.5 Awareness, training and security checks in relation to personnel;

2.1.6 Incident/Response Management/Business Continuity; and

2.1.7 Audit Controls/Due Diligence;

---

1 The Practical Security Measures outlined in Schedule 1 are taken from the OECD Working Party on Information Security and
Privacy's draft paper of 30-31March 2004 entitled "Information Security Issues and Resources for Small and Entrepreneurial
Companies – A business companion to the 2002 OECD Guidelines for the Security of Networks and Information systems:
Towards a Culture of Security"

Annex A (normative):
Article 17 Security Contract - Implementation Guide

AA.1 **Scope**

The Article 17 Security Contract has been prepared to assist businesses wishing to use the services of another company to process personal data on their behalf. The Article 17 Security Contract is appropriate for use where the company which is to provide the data processing service is located either in the same Member State as the business wishing to use its services or, is located another Member State of the European Union.

Article 17 of the Directive sets out the security requirements in relation to the processing of personal data where a party that controls the content and use of personal data (the Data Controller) wishes to use the services of a third party (the Data Processor) for the processing of such data. Article 17 addresses processing arrangements where both the Data Controller and the Data Processor are established within one of the member states of the European Economic Area.

Where the Data Processor is located outside the European Economic Area consideration will need to be given to the provisions of Articles 25 and 26 of the Directive (Transfer of Personal Data to Third Countries) and the possible use of the Standard Contractual Clauses for the transfer of personal data to third countries under the Directive approved by the European Commission.

The Article 17 Security Contract has been prepared with the needs of Small and Medium-sized Enterprises in mind, however, it may in addition provide a useful starting point for larger organisations wishing to ensure that they are satisfying their obligations as to security of processing where they sub-contract data processing to another company.

The Article 17 Security Contract has been drafted to satisfy the requirements of Article 17 and is unlikely to
require amendment in the absence of any changes to that Article. The contractual provisions set out in the Security Contract ensure the basic minimum level of protection for personal data and do not preclude the inclusion of more detailed provisions in the light of the legal and factual circumstances of each particular case.

However, the practical security measures suggested in this Implementation Guide are likely to require amendment in the light of physical and technological security developments and the adoption of enhanced management functions in relation to information security. This Implementation Guide, therefore, sets out the current practical security measures identified at the time of drafting, taking into account the most common technical security measures currently available, but may subsequently require updating to incorporate future developments.

The Article 17 Security Contract is designed to accompany a service agreement detailing the non-security related processing arrangements between the Data Controller and the Data Processor. The Contract may be used in its entirety or the operative clauses may be extracted and incorporated into the processing service agreement.

Before entering in an Article 17 Security Contract, or the data processing services agreement into which the operative of the Security Contract have been incorporated, the parties should obtain the assistance of professional legal advisers (in-house or external lawyers) for advice on the requirements of the national law (including any sector specific regulatory arrangements) to which the contract and the associated processing will be subject.

This guide provides assistance with regard to the use of the Article 17 Security Contract between Data Controller and Data Processor.

AA.2 **Background**

The Initiative for Privacy Standardisation in Europe (IPSE) was launched to analyse the current status of privacy protection arrangements and to determine whether standardisation of actions could assist business in implementing the European Data Protection Directive 95/46/EC (the Directive). The report, approved by the IPSE steering group, concluded that specific standardisation initiatives would aid implementation of the Directive. Seven standardisation initiatives were proposed, one of which was the development of a generic set of contract clauses and terms for use within the EEA to assist business in complying with Article 17 of the Directive.

The work on the standardisation initiatives identified by IPSE was taken on by the CEN/ISSS Work Shop on Data Protection and Privacy (CEN/ISSS WS-DPP) which has produced the Article 17 Security Contract between Data Controller and Data Processor.

AA.3 **Applicable Laws**

Clause 6 of the Security Contract provides that the Agreement is to be governed by the national law of the Member State in which the Data Controller is located.

Where the Data Processor is located in a different Member State from the Data Controller the Controller should note that the security of the processing may be governed by the laws of a different Member State. This situation arises as (in accordance with the provisions of Article 17) the security of the processing must be conducted in accordance with the national law of the Member State in which the Data Processor is located.

Where the Data Processor is located in a Member State other than that of the Data Controller, prior to entering into contractual relations with the Data Processor, the Data Controller may need to obtain legal advice as to the specific foreign law data protection obligations imposed on the Data Processor under Clause 3 of the Model Contract. Where the Data Controller fails to obtain foreign legal advice the Data Controller may struggle to assess the Data Processor's compliance with its Clause 3 obligations. While the obligations of the Data Processor, in each Member State, derive from Article 17 of the Directive, Member States have each implemented these obligations slightly differently. For example, in many Member States (such as Austria, Belgium, Ireland, Italy, Luxembourg and Spain) the security provisions under the national law are more detailed than in the Data Protection Directive. The Data Processor will, therefore, need ensure that it complies with the provisions under the applicable national law.

In certain Member States there are regulations detailing mandatory security measures which identify three differing levels of security determined by the nature of the data being processed.

High level security measures required in Spain include, amongst other requirements, strict obligations regarding the encryption of personal data in specified circumstances as well as the maintenance of an exhaustive access registry. The Spanish access register requires a Controller to specify the data accessed by any user and the date and time of such access so as to enable the reconstruction of an audit trail in relation to access to sensitive personal data.

In Belgium, national data protection legislation stipulates and number of issues that must be covered in any
sub-contracting agreement between Data Controller and Data Processor. Such issues include a requirement that the agreement shall explicitly include details of the processors liability under the agreement. The Belgium law also provides that a Royal Decree may be enacted to establish standards for information security for specified categories of data processing.

In Greece the national data protection law requires the Data Controller to check the professional credentials, qualifications and personal ethics with regard to confidentiality of persons entrusted with data processing duties or functions.

In addition to these specific national legal requirements some national data protection authorities (for example Greece and Denmark) have established rules, instructions and guidelines translating into more practical terms some of the requirements of Article 17.

AA.4 Clause by clause explanatory notes/analysis of the Article 17 Security Contract

As with any arrangement having binding legal effect, users of the Article 17 Security Contract are advised to seek professional legal advice with regard to their rights and obligations under the Security Contract and its inter relationship with any associated data processing service agreement.

Professional legal input is particularly important where the Data Controller is uncertain of the obligations imposed on the Data Processor under the Processor's national law.

The following notes are intended as basic guidance on the nature and purpose of the individual clauses of the Security Contract and are intended to inform business managers understanding of the Security Contract prior to obtaining detailed legal advice.

Contract Clauses

Date of Agreement

The date of the agreement will be the date on which the last party executes the document. This date should not be inserted until the last party has signed and dated the Contract.

Identification of Parties

The full name of the legal entities entering into the agreement should be inserted together with any nationalcompany registration number, details of the country in which each legal entity is established and details of the registered office of each entity. It is important to note that address must be the registered office address of each business. Trading addresses, or local office addresses should not be used.

Background

The six paragraphs listed under this heading set out the reasons why the agreement is required. They identify the activities of the parties, the processing of personal data, the parties who wish to enter into contractual relations with one another, and the requirements of Article 17 of the Directive.

Mutual Agreement

The Contract then states that the parties agree to comply the provisions of the Contract.

Clause 1 – Definitions and Interpretation

This clause explains the meaning of those terms used in the agreement which have meaning over and
above, or different from, the meaning which may normally be understood by the use of the term. For
example, the words "personal data" are to have the specific meaning ascribed to them by the Directive.

Clause 2 – Consideration

Broadly speaking this clause is required to set out the reasons why each party is prepared to enter into the agreement. The Contract arrangement needs to be of benefit to (or, in legal terms, provide valid consideration) each party.

Clause 3 – Security Obligations of the Processor

As the title of this clause would suggest, it sets out the security obligations of the Data Processor with regard to the processing of personal data on behalf of the Data Controller.

Important points to note are:

- the Processor may only process personal data in accordance with instructions from the Data Controller. It may not process the data for its own purposes;

- the Processor is required to take "such Technical and Organisation Security Measures as are required under **its own National Law** to protect personal data processed on behalf of the Data Controller against unlawful forms of processing". As mentioned above, legal advice should be obtained as to the detailed requirements of the relevant national law; and

- Appendix 1 of the Contract sets out the minimum requirements for compliance with these obligations. Appendix 1 is discussed further below.

Clause 4 – Confidentiality

This clause ensures that the Processor must treat all personal data processed on behalf of the Data
Controller as confidential and provides that the obligation of confidentiality is continue for 5 years after the date on which the Processor ceases processing personal data for the Controller. This time limit is without prejudice to any longer time-limits that may be provided by national law or sector specific regulation. The parties may wish to amend this provision to reflect such additional obligations.

Clause 5 – Sub-contracting

This clause prevents the Processor from instructing a third party to carry out the processing it has agreed to carry out for the Controller unless the Controller gives its prior written consent.

Where the Controller consents to the sub-contracting, the sub-contractor must be contractually bound to
observe the same security requirements as are imposed on the Processor under the Security Contract.

This clause ensures that the security arrangements are not watered-down by any transfer of obligations. The clause also provides that the Processor remains liable to the Controller for any breach of the Security Contract whether caused by any fault of its own or by the fault of its sub-contractor.

Clause 6 – Term and termination

This clause provides that the Security Contract will continue for as long as the Processor continues to
process personal data on behalf of the Controller. The Security Contract cannot terminate before the data processing service agreement as any subsequent processing would not comply with Article 17.

Where the Security Contract and the data processing agreement are terminated, clause 5.2 provides that the Processor shall return or destroy all personal data received from the Controller as instructed by the Controller. It is for the parties to agree the appropriate number of days to insert in the clause.

This arrangement is fallback position to specify arrangements for the handling of the personal data on

termination where there are no other arrangements in place. It is highly likely that the termination arrangements will be addressed in the data processing service agreement but clause 5.2 is available as
backup if such arrangements have been overlooked in the drafting of the service agreement.

Clause 7 – Governing law

The Security Contract provides that the contract is to be governed by the National Law of the Data Controller.

Care must be taken when considering the choice of governing law in circumstances where the data processing service agreement specifies a law other than that of the Member State of the Controller as its governing law. In such circumstances professional legal advice may be required.

The Security Contract does not address dispute resolution. It is advisable, before the Contract is signed, for the parties to agree an appropriate forum to hear any disputes that may arise between them under the Contract. Many parties may favour mediation with recourse to specified national courts if matters cannot be resolved. Others may wish to specify arbitration as the preferred dispute resolution process. Where mediation or arbitration are to be used it is advisable to identify the chosen mediator (or mediation body) or arbitration procedure in writing so as to avoid a dispute about the Contract becoming a dispute about the resolution procedure.

As the Security Contract is to be used in association with a data processing service agreement it may be appropriate to deal with dispute resolution arrangements in relation to security obligations under the service agreement or to mirror the dispute resolution arrangements under the service agreement in the Security Contract. Where mediation or arbitration is not specified, as a minimum, the parties should agree to submit to the exclusive jurisdiction of specified national courts to avoid any further discussion as to where disputes should be heard. It is usual for parties to agree to submit to the exclusive jurisdiction of the courts appropriate to the governing law of the contract.

Signature

Both parties should ensure that the Contract is executed on their behalf by a ‘duly authorised representative’. That is to say the parties should ensure that the signatories have the power to bind the organisation they represent. In many jurisdictions, in the absence of any other arrangements being made, the only individuals authorised to bind a company will be the directors and company secretary. These individuals may of course give written authority to other employees to bind the company for specified purposes. The identity and the authority of the proposed signatory should always be confirmed before attempting to enter into contractual relations.

Appendix 1

This appendix sets out the minimum technical and organisational measures to be observed by the Processor in accordance with clause 3. The appendix is divided into Legal Requirements and Practical Security Measures.

The Legal Requirements

These relate to the need for the Data Processor to identify and observe any specific security measures in relation to personal data required under its national law. The requirement is not a one-off requirement to be observed at the start of the processing service, but is an on-going obligation to ensure that the security arrangements are in compliance with national law as it may be amended or supplemented from time to time throughout the duration of the processing service.

Practical Security Measures

While the Contract imposes the obligation on the Processor to take “such Technical and Organisation

Security Measures as are required under its own National Law to protect personal data processed on behalf of the Data Controller against unlawful forms of processing" many businesses may find it difficult to ascertain what this obligation means in practice.

The obligation is a broad one and businesses will need to break this down into the classes of security
measures identified in the appendix. These classes will require further practical consideration. Many
international IT groups and standards bodies have looked at the area of information security and guidance of general application is available from many of the bodies referred to below (see Sources).

An example of appropriate basic information security measures are set out in Annex 1 of this Implementation Guide.

AA.5 Extra Clauses

The Security Contract (whether used as an separate agreement or with extracted clauses used to supplement a data processing agreement) is intended to satisfy the requirements of Article 17.

From a business perspective, however, where such matters have not been otherwise covered in the data processing agreement or related contract, parties may wish to include additional clauses regarding, for example:

- Arbitration or mediation arrangements (as discussed above);
- Selection of jurisdiction (as discussed above);
- Limitations of liability.

Where more detailed arrangements have not been dealt with in other agreements, parties may wish to include more detailed provisions in relation to some of the matters addressed in the Security Contract, for example:

- Arrangements for the treatment of personal data on termination of the processing arrangements.

AA.6 Sources

The following bodies provide helpful guidance and information on information security, privacy enhancing
technologies and data protection and privacy considerations which may serve as useful additional reading material for organisations seeking to use the Article 17 Security Contract for the first time:

- OECD/EU
- National Bodies
- BCS, ITIL
- ICC (International Chamber of Commerce)
- ISO 17799
- Common Criteria
- PETTEP

IMPLEMENTATION GUIDE

ANNEX 1 - BASIC INFORMATION SECURITY MEASURES

Basic information security measures (here extracted from work of the OECD) will include consideration of the following:

2.1 Information Security Management System/Privacy and Data Protection Management System

- Policy
- Governance

- Process/procedures
- Roles/responsibilities
- Assurance process
- Risk Assessment
- Improvement plan.

2.2 Physical Security

- Fit appropriate locks or other physical controls to the doors and windows of rooms where computers are kept.
- Physically secure unattended lap tops (for example, by locking them in a secure drawer or cupboard).
- Ensure you control and secure all removable media, such as removable hard-drives, CDs, floppy disks and USB drives, attached to business-critical assets.
- Destroy or remove all business-critical information from media such as CDs, and floppy disks before disposing of them.
- Ensure that all business-critical information is removed from the hard drives of any used computers before disposing of them.
- Store back-ups of business-critical information either off-site or in a fire and water-proof container.

2.3 Access Controls

- Use unique passwords, that are not obvious *(*Note: not birth dates or easily found or guessed information*)* and change them regularly *(*Note: preferably at least every three months*).*
- Use passwords that contain letters in both upper and lower cases, numbers and special keys, and are six or more characters in length. (Note: Passwords remembered as a memorable sentence, rather than a single word, are helpful. For example, the sentence: “at forty-two I’m a star!” can translate into this eight-character password : @42Ima**!)*
- Ensure that employees don’t write down or share passwords. *(*Note: If an employee finds that they need, on occasion, to share a password they must be required to change it as soon as possible – no matter how well they trust the person they shared it with!*)*

2.4 Security and Privacy Technologies

- Ensure that all computers used have anti-virus software installed, and the virus definitions must be updated at least once a week *(*Note: many providers have a one-click update*).* Allincoming and outgoing traffic must be scanned for viruses, as should any disk or CD that is used, even if it is from a ‘trusted’ source. At least once a month, computers must be scanned for viruses.

- Where computers are connected to the Internet (especially if you use a broadband connection) deploy a software firewall. *(*Note: This helps to prevent malicious code from entering computers and potentially compromising the confidentiality, integrity and availability of a network. It also helps to stop a system being used to attack other systems without the system owner’s knowledge. Software firewalls for use by non-professionals are readily available at a reasonable cost. Operating system virus control software or ISPs may also offer firewalls. Consumer and popular trade magazines compare firewall functions and features of well known products, and are a good source of information. Free shareware firewalls are available, but these usually require expert knowledge for correct use*).*

- Where a business has a small network that is connected to the Internet, it should consider deploying an ‘all-in-one’ hardware box that contains a firewall, anti-virus program and an intrusion detection system. *(*Note: This will greatly simplify the use and maintenance of essential Internet security technology*).*

2.5 Awareness, training and security checks in relation to personnel

- Perform integrity checks on all new employees to ensure that they have not lied about their background, experience or qualifications.
- Give all new employees a simple introduction to information security, and ensure that they read and understand your information security policy. Ensure employees know where to find details of the information security standards and procedures relevant to their role and responsibilities.
- Ensure that employees have access only to the information assets they need to do their jobs. If employees change jobs, you must ensure that they do not retain access to the assets they needed for their old job. When dismissing employees, ensure that they do not take with them any business-critical information.
- Ensure that no ex-employees have access rights to your systems.
- Ensure employees know about the common methods that can be used to compromise your system. *(*Note: These include e-mail messages that contain viruses and 'social engineering' ploys used by hackers to exploit employees' helpfulness to gain information that will give them access to a system. Examples of 'social engineering' include a hacker using the telephone to pose as a systems maintenance engineer or pretending to be a new employee*).*

2.6 Incident/Response Management/Business Continuity

- Ensure that employees understand what is meant by a Security Incident. A security incident is any event that can damage or compromise the confidentiality, integrity or availability of your business–critical information or systems.

- Ensure that employees are trained to recognise the signs of Security Incidents. (*Note: These could include:*

    - strange phone requests, especially for information
    - unusual visitors
    - strange patterns of computer activity
    - unusual appearance of computer screens
    - computers taking longer than usual to perform routine tasks*)*
    - Ensure that employees receive training on the need to notify anything which may be a sign of a Security Incident and are kept informed as to the identity of the person to whom such notifications should be made.
- Ensure that if a Security Incident occurs, employees know who to contact and how.
- Have in place a plan to assure business continuity in the event of a serious Security Incident (a "Business Recovery Plan"). The plan should specify:
- Designated people involved in the response;
- External contacts, including law enforcement, fire and possibly technical experts;
- Contingency plans for foreseeable incidents such as:
  o Power loss;
  o Natural disasters and serious accidents;
  o Data compromise;
  o No access to premises;
  o Loss of essential employees;
  o Equipment failure;

- Ensure that your Business Recovery Plan is issued to all employees and is tested at least once a year, regardless of whether there has been a Security Incident.
- After every incident when the plan is used, and after every test, re-examine and update the Business Recovery Plan as necessary using the lessons learned.

2.7 Audit Controls/Due Diligence

Ensure that you have in place appropriate security audit arrangements including:

- Auditing of who has access to its system (in general and in relation to particular types of information) *(*Note: The ability to audit and evaluate information security compliance is essential – you can't manage what you don't measure!*);*
- Logging of such access to the system; and
- Auditing of compliance with security procedures. *(*Note: A record should be maintained for each security procedure. For example, if a procedure requires that you test your system's back-up generator once a week, an employee should be identified to sign a record to show that this has been done. Keeping good records is essential to audit control*.)*

Some audit controls may be necessary for legal or regulatory purposes. Good record keeping will clearly demonstrate compliance with obligations.

An audit should ensure that the procedures in place are effective and relevant. A security audit is a trigger to re-assess and re-evaluate the effectiveness of information security standards and procedures.

Audits are only effective if action is taken to address their findings and identify and implement the steps that need to be taken. A good audit trail is not just a paper exercise. If something goes wrong, the trail should identify what happened and why. This will help to keep improving the security of the business systems.

ANNEX 1: DATA SHARING PROTOCOL

[NOTE: DATA SHARING PROTOCOL TO BE INSERTED FOLLOWING CONTRACT AWARD DEPENDING ON DATA TRANSFER REQUIREMENTS AND DETAILS BEING FINALISED.]

This and the following 10 pages comprise Schedule 10 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 10 – EXIT MANAGEMENT

1. **DEFINITIONS**

1.1 In this Schedule, the following definitions shall apply:

"**Exclusive Assets**" means those Service Provider Assets used by the Service Provider or a Key Sub-Contractor which are used exclusively in the provision of the Services;

"**Exit Information**" has the meaning given to it in paragraph 4.1 of this Schedule;

"**Exit Manager**" means the person appointed by each Party pursuant to paragraph 3.4 of this Schedule for managing the Parties' respective obligations under this Schedule;

"**Key Sub-Contractor**" means each Sub-contractor listed in Schedule 6 and any additional sub-contractors who are notified to and approved by the Purchaser pursuant to the Contract;

"**Net Book Value**" means the net book value of the relevant Service Provider Asset(s) calculated in accordance with the depreciation policy of the Service Provider set out in the letter in the agreed form from the Service Provider to the Purchaser of even date with this Contract;

"**Non-Exclusive Assets**" means those Service Provider Assets (if any) which are used by the Service Provider or a Key Sub-Contractor in connection with the Services but which are also used by the Service Provider or Key Sub-Contractor for other purposes;

"**Purchaser Data**" means any data (including any Personal Data (as defined in section 1(1) of the Data Protection Act 1998) relating to the staff, customers or suppliers of the Purchaser), documents, text, drawings, diagrams, images or sounds (together with any database made up of any of those), embodied in any medium, that are supplied to the Service Provider by or on behalf of the Purchaser, or which the Service Provider is required to generate, process, store or transmit pursuant to the Contract;

"**Purchaser Software**" means any software which is used by, or licensed to, the Purchaser other than pursuant to the Contract, and which may be used by the Service Provider for the sole purpose of providing the Services to the Purchaser;

"**Registers**" means the register and configuration database referred to in paragraphs 3.1.1 and 3.1.2 of this Schedule;

"**Service Provider Assets**" means all assets and rights of the Service Provider which are required to provide any of the Services in accordance with the Contract;

"**Sub-Contracts**" means any contract between the Service Provider and a third party pursuant to which the Service Provider agrees to source the provision of any of the Services from that third party;

"**Termination Assistance**" means the activities to be performed by the Service Provider pursuant to the Exit Plan, and any other assistance required by the Purchaser pursuant to the Termination Assistance Notice;

"**Termination Assistance Notice**" has the meaning given to it in paragraph 6.1 of this Schedule;

"**Termination Assistance Period**" means in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Service Provider is required to provide the Termination Assistance as such period may be extended pursuant to paragraph 6.2 of this Schedule;

"**Termination Notice**" a written notice of termination given by one Party to the other, notifying the Party receiving the notice of the intention of the Party giving the notice to terminate this Contract (in whole or in part) on a specified date and setting out the grounds for termination.

"**Third Party Software**" means software which is proprietary to any third party and that is either licensed to the Purchaser or is used by the Service Provider in the provision of the Services, but excluding any Purchaser Software;

"**Transferable Assets**" means those of the Exclusive Assets which are capable of legal transfer to the Purchaser;

"**Transferable Contracts**" means the Sub-Contracts, licenses for Service Provider 's software, licenses for Third Party Software or other agreements which are necessary to enable the Purchaser or any Replacement Service Provider to perform the Services (or any replacement to the Services), including in relation to licenses all relevant Documentation;

"**Transferring Assets**" has the meaning given to it in paragraph 9.2.1 of this Schedule;

"**Transferring Contracts**" has the meaning given to it in paragraph 9.2.3 of this Schedule.

2. **INTRODUCTION**

2.1 This Schedule describes provisions that should be included in the Exit Plan, the duties and responsibilities of the Service Provider to the Purchaser leading up to and covering the transfer of service provision to the Purchaser and/or a Replacement Service Provider.

2.2 The objectives of the exit planning and service transfer arrangements are to ensure a smooth transition of the availability of the Services (in whole or in part) from the Service Provider to the Purchaser and/or a Replacement Service Provider.

3. **OBLIGATIONS DURING THE CONTRACT PERIOD TO FACILITATE EXIT**

3.1 During the Contract Period, the Service Provider shall:

3.1.1 create and maintain a Register of all:

(a) Sub-Contracts and other relevant agreements (including relevant software licenses, maintenance and support agreements and equipment rental and lease agreements) required for the performance of the Services; and

(b) Exclusive Assets and Non-Exclusive Assets.

3.1.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Service Provider provides the Services, which shall contain sufficient detail to permit the Purchaser and/or Replacement Service Provider to understand how the Service Provider provides the Services and to enable the smooth transition of the Services with the minimum of disruption;

3.1.3 agree the format of the Registers with the Purchaser as part of the process of agreeing the Exit Plan; and

3.1.4 at all times keep the Registers up to date, in particular in the event that Assets (whether Exclusive or Non-Exclusive), Sub-Contracts or other relevant agreements are added to or removed from the Services.

3.2 The Service Provider shall:

3.2.1 procure that all Exclusive Assets listed in the Registers are clearly marked to identify that they are exclusively used for the provision of the Services under this Contract; and

3.2.2 (unless otherwise agreed by the Purchaser in writing) procure that all licenses for Third Party Software and all Sub-Contracts shall be assignable and/or capable of novation at the request of the Purchaser to the Purchaser (and/or its nominee) and/or any Replacement Service Provider upon the Service Provider ceasing to provide the Services (or part of them) without restriction (including any need to obtain any consent or approval) or payment by the Purchaser.

3.3 Where the Service Provider is unable to procure that any Sub-Contract or other agreement referred to in paragraph 3.2.2 of this Schedule which the Service Provider proposes to enter into after the Effective Date is assignable and/or capable of novation to the Purchaser (and/or its nominee) and/or any Replacement Service Provider without restriction or payment, the Service Provider shall promptly notify the Purchaser of this and the Parties shall (acting reasonably and without undue delay) discuss the appropriate action to be taken which, where the Purchaser so directs, may include the Service Provider seeking an alternative Sub-Contractor or provider of goods and/or services to which the relevant agreement relates.

3.4 Each Party shall appoint a person (the "**Exit Manager**") for the purposes of managing the Parties' respective obligations under this Schedule and provide written notification of such appointment to the other Party within three (3) months of the Effective Date. The Service Provider's Exit Manager shall be responsible for ensuring that the Service Provider and its employees, agents and Sub-Contractors comply with this Schedule. The Service Provider shall ensure that its Exit Manager has the requisite authority to arrange and procure any resources of the Service Provider as are reasonably necessary to enable the Service Provider to comply with the requirements set out in this Schedule. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the termination of this Contract and all matters connected with this Schedule and each Party's compliance with it.

4. **OBLIGATIONS TO ASSIST ON RE-TENDERING OF SERVICES**

4.1 On reasonable notice at any point during the Contract Period, the Service Provider shall provide to the Purchaser and/or its potential Replacement Service Providers (subject to the potential Replacement Service Provider s entering into reasonable written confidentiality undertakings), the following material and information in order to facilitate the preparation by the Purchaser of any invitation to tender and/or to facilitate any potential Replacement Service Providers undertaking due diligence:

4.1.1 details of the Service(s);

4.1.2 a copy of the Registers, updated by the Service Provider up to the date of delivery of such Registers;

4.1.3 an inventory of Purchaser Data in the Service Provider 's possession or control;

4.1.4 details of any key terms of any third party contracts and licenses, particularly as regards charges, termination, assignation and novation;

4.1.5 a list of on-going and/or threatened disputes in relation to the provision of the Services;

4.1.6 all information relating to transferring Service Provider's Representatives required to be provided by the Service Provider under this Contract; and

4.1.7 such other material and information as the Purchaser shall reasonably require,

(together, the "**Exit Information**").

4.2 The Service Provider acknowledges that the Purchaser may disclose the Service Provider Sensitive Information (or any other information, whether confidential or otherwise) to an actual or prospective Replacement Service Provider or any third party whom the Purchaser is considering engaging to the extent that such disclosure is necessary in connection with such engagement (except that the Purchaser may not under this paragraph 4.2 of this Schedule disclose any such information where and to the extent that it relates to the Service Provider's or its Sub-Contractors' prices or costs).

4.3 The Service Provider shall:

4.3.1 notify the Purchaser within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Services and shall consult with the Purchaser regarding such proposed material changes; and

4.3.2 provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and in any event within ten (10) Working Days of a request in writing from the Purchaser.

4.4 The Service Provider may charge the Purchaser for its reasonable additional costs to the extent the Purchaser requests more than four (4) updates in any six (6) month period.

4.5 The Exit Information shall be accurate and complete in all material respects and the level of detail to be provided by the Service Provider shall be such as would be reasonably necessary to enable a third party to:

4.5.1 prepare an informed offer for those Services; and

4.5.2 not be disadvantaged in any subsequent procurement process compared to the Service Provider (if the Service Provider is invited to participate).

5. **EXIT PLAN**

5.1 The Service Provider shall, within three (3) months after the Effective Date, deliver to the Purchaser an Exit Plan which:

5.1.1 sets out the Service Provider 's proposed methodology for achieving an orderly transition of the Services from the Service Provider to the Purchaser and/or its Replacement Service Provider on the expiry or termination of this Contract;

5.1.2 complies with the requirements set out in paragraph 5.3 of this Schedule;

5.1.3 is otherwise reasonably satisfactory to the Purchaser.

5.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of its submission, then such dispute shall be resolved in accordance with the Management Arrangements.

5.3 Unless otherwise specified by the Purchaser, the Exit Plan shall set out, as a minimum:

5.3.1 how the Exit Information is obtained;

5.3.2 the management structure to be employed during both transfer and cessation of the Services;

5.3.3 the management structure to be employed during the Termination Assistance Period;

5.3.4 a detailed description of both the transfer and cessation processes, including a timetable;

5.3.5 how the Services will transfer to the Replacement Service Provider and/or the Purchaser, including details of the processes, documentation, data transfer, systems migration, security and the segregation of the Purchaser's technology components from any technology components operated by the Service Provider or its Sub-Contractors (where applicable);

5.3.6 details of contracts (if any) which will be available for transfer to the Purchaser and/or the Replacement Service Provider together with any reasonable costs required to effect such transfer (and the Service Provider agrees that all assets and contracts used by the Service Provider in connection with the provision of the Services will be available for such transfer);

5.3.7 proposals for the training of key individuals of the Replacement Service Provider's personnel in connection with the continuation of the provision of the Services charged at rates agreed between the Parties (each acting reasonably) at that time;

5.3.8 proposals for providing the Purchaser or a Replacement Service Provider copies of all documentation:

(a) used in the provision of the Services and necessarily required for the continued use thereof, in which the Intellectual Property Rights are owned by the Service Provider; and

(b) relating to the use and operation of the Services;

5.3.9 proposals for the assignation or novation of the provision of all services, leases, maintenance agreements and support agreements utilised by the Service Provider in connection with the performance of the supply of the Services to the extent required by the Purchaser or any Replacement Service Provider;

5.3.10 proposals for the identification and return of all Purchaser property in the possession of and/or control of the Service Provider or any third party (including any Sub-Contractor);

5.3.11 proposals for the disposal of any redundant Services and materials;

5.3.12 procedures to deal with requests made by the Purchaser and/or a Replacement Service Provider for information in respect of any Service Provider Representatives;

5.3.13 how each of the issues set out in this Schedule will be addressed to facilitate the transition of the Services from the Service Provider to the Replacement Service Provider and/or the Purchaser with the aim of ensuring that there is no disruption to or degradation of the Services during the Termination Assistance Period; and

5.3.14 proposals for the supply of any other information or assistance reasonably required by the Purchaser or a Replacement Service Provider in order to effect an orderly handover of the provision of the Services.

5.4 The Service Provider shall throughout the Contract Period review, and maintain the Exit Plan. If the Service Provider believes that any updates are required to the Exit Plan it shall provide written notification to the Purchaser outlining the details of any proposed updates. The Parties shall use reasonable endeavours to agree the contents of any updates to the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of its submission, then such dispute shall be resolved in accordance with the Management Procedures.

6. **TERMINATION ASSISTANCE**

6.1 The Purchaser shall be entitled to require the provision of Termination Assistance at any time during the Contract Period by giving written notice to the Service Provider (a "**Termination Assistance Notice**") at any time prior to the end of the contract following the service by either Party of a Termination Notice. The Termination Assistance Notice shall specify:

6.1.1 the date from which Termination Assistance is required;

6.1.2 the nature of the Termination Assistance required; and

6.1.3 the period during which it is anticipated that Termination Assistance will be required ("**Termination Assistance Period**"), which shall continue no longer than twelve (12) months after the date that the Service Provider ceases to provide the Services.

6.2 The Purchaser shall have an option to extend the Termination Assistance Period beyond the period specified in the Termination Assistance Notice provided that such extension shall not extend for more than six (6) months beyond the end of the Termination Assistance Period and provided that it shall notify the Service Provider to such effect no later than twenty (20) Working Days prior to the date on which the provision of Termination Assistance is otherwise due to expire. The Purchaser shall have the right to terminate its requirement for Termination Assistance by serving not less than (20) Working Days' written notice upon the Service Provider to such effect.

7. **TERMINATION ASSISTANCE PERIOD**

7.1 Throughout the Termination Assistance Period, or such shorter period as the Purchaser may require, the Service Provider shall:

7.1.1 continue to provide the Services and, if required by the Purchaser pursuant to paragraph 6.1 of this Schedule, provide the Termination Assistance;

7.1.2 in addition to providing the Services and the Termination Assistance, provide to the Purchaser any reasonable assistance requested by the Purchaser to allow the Services to continue without interruption following the termination or expiry of this Contract and to facilitate the orderly transfer of responsibility for and conduct of the Services to the Purchaser and/or its Replacement Service Provider;

7.1.3 use all reasonable endeavours to reallocate resources to provide such assistance as is referred to in paragraph 7.1.2 of this Schedule without additional costs to the Purchaser;

7.1.4 provide the Services and the Termination Assistance at no detriment to the Service Levels , save to the extent that the Parties agree otherwise in accordance with paragraph 7.3; and

7.1.5 at the Purchaser's request and on reasonable notice, deliver up-to-date Registers to the Purchaser.

7.2 Without prejudice to the Service Provider's obligations under paragraph 7.1.3 of this Schedule, if it is not possible for the Service Provider to reallocate resources to provide such assistance as is referred to in paragraph 7.1.2 of this Schedule without additional costs to the Purchaser, any additional costs incurred by the Service Provider in providing such reasonable assistance which is not already in the scope of the Termination Assistance or the Exit Plan shall be subject to the Change Control Procedure.

7.3 If the Service Provider demonstrates to the Purchaser's reasonable satisfaction that transition of the Services and provision of the Termination Assistance during the Termination Assistance Period will have a material, unavoidable adverse effect on the Service Provider 's ability to meet one or more particular Service Levels , the Parties (each acting reasonably) shall discuss and endeavour to agree a variation to the relevant Service Level(s) to take account of such adverse effect.

8. **TERMINATION OBLIGATIONS**

8.1 The Service Provider shall comply with all of its obligations contained in the Exit Plan.

8.2 Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Service Provider 's performance of the

Services and the Termination Assistance and its compliance with the other provisions of this Schedule), the Service Provider shall:

8.2.1 cease to use the Purchaser Data;

8.2.2 provide the Purchaser and/or the Replacement Service Provider with a complete and uncorrupted version of the Purchaser Data in (an open) electronic form (or such other format as reasonably required by the Purchaser);

8.2.3 erase from any computers, storage devices and storage media that are to be retained by the Service Provider after the end of the Termination Assistance Period all Purchaser Data and promptly certify to the Purchaser that it has completed such deletion;

8.2.4 return to the Purchaser such of the following as is in the Service Provider 's possession or control:

(a) all copies of the Purchaser Software and any other software licensed by the Purchaser to the Service Provider under this Contract;

(b) all materials created by the Service Provider under this Contract in which the Intellectual Property Rights are owned by the Purchaser;

(c) any items that have been on-charged to the Purchaser, such as consumables; and

(d) all Purchaser Property issued to the Service Provider. Such Purchaser Property shall be handed back to the Purchaser in good working order (allowance shall be made only for reasonable wear and tear);

(e) any sums prepaid by the Purchaser in respect of Services not delivered by the Expiry Date;

8.2.5 provide access during normal working hours to the Purchaser and/or the Replacement Service Provider for up to twelve (12) months after expiry or termination to:

(a) such information relating to the Services as remains in the possession or control of the Service Provider; and

(b) such members of the Service Provider Representatives as have been involved in the design, development and provision of the Services and who are still employed by the Service Provider, provided that the Purchaser and/or the Replacement Service Provider shall pay the reasonable costs of the Service Provider actually incurred in responding to requests for access under this paragraph.

8.3 Upon termination or expiry (as the case may be) or at the end of the Termination Assistance Period (or earlier if this does not adversely affect the Service Provider 's performance of the Services and the Termination Assistance and its compliance with the other provisions of this Schedule), each Party shall return to the other Party (or if requested, destroy or delete) all confidential information of the other Party (including the Purchaser Protected Information and the Service Provider Sensitive Information) and shall certify that it does not retain such information save to the extent (and for the limited period) that such information needs to be retained by the Party in question for the purposes of providing or receiving any Services or termination services or for statutory compliance purposes.

8.4 Except where this Contract provides otherwise, all licences, leases and authorisations granted by the Purchaser to the Service Provider in relation to the Services shall be terminated with effect from the end of the Termination Assistance Period.

9. **ASSETS, SUB-CONTRACTS AND SOFTWARE**

9.1 Following notice of termination of this Contract and during the Termination Assistance Period, the Service Provider shall not, without the Purchaser's prior written consent:

9.1.1 terminate, enter into or vary any Sub-Contract;

9.1.2 (subject to normal maintenance requirements) make material modifications to, or dispose of, any existing Service Provider Assets or acquire any new Service Provider Assets; or

9.1.3 terminate, enter into or vary any license for software in connection with the provision of Services.

9.2 Within twenty (20) Working Days of receipt of the up-to-date Registers provided by the Service Provider pursuant to paragraph 7.1.5 of this Schedule, the Purchaser shall provide written notice to the Service Provider setting out:

9.2.1 which, if any, of the Transferable Assets the Purchaser requires to be transferred to the Purchaser and/or the Replacement Service Provider ("**Transferring Assets**");

9.2.2 which, if any, of:

(a) the Exclusive Assets that are not Transferable Assets; and

(b) the Non-Exclusive Assets,

the Purchaser and/or the Replacement Service Provider requires the continued use of; and

9.2.3 which, if any, of Transferable Contracts the Purchaser requires to be assigned or novated to the Purchaser and/or the Replacement Service Provider (the "**Transferring Contracts**"), in order for the Purchaser and/or its Replacement Service Provider to provide the Services from the expiry of the Termination Assistance Period. Where requested by the Purchaser and/or its Replacement Service Provider, the Service Provider shall provide all reasonable assistance to the Purchaser and/or its Replacement Service Provider to enable it to determine which Transferable Assets and Transferable Contracts the Purchaser and/or its Replacement Service Provider requires to provide the Services.

9.3 With effect from the expiry of the Termination Assistance Period, the Service Provider shall sell the Transferring Assets to the Purchaser and/or its nominated Replacement Service Provider for a consideration equal to their Net Book Value, except where the cost of the Transferring Asset has been partially or fully paid for through the Contract Charges at the end of contract, in which case the Purchaser shall pay the Service Provider the Net Book Value of the Transferring Asset less the amount already paid through the Contract Charges.

9.4 Risk in the Transferring Assets shall pass to the Purchaser or the Replacement Service Provider (as appropriate) at the end of the Termination Assistance Period and title to the Transferring Assets shall pass to the Purchaser or the Replacement Service Provider (as appropriate) on payment for the same.

9.5 Where the Service Provider is notified in accordance with paragraph 9.2.2 of this Schedule that the Purchaser and/or the Replacement Service Provider requires continued use of any Exclusive Assets that are not Transferable Assets or any Non-Exclusive Assets, the Service Provider shall as soon as reasonably practicable:

9.5.1 procure a non-exclusive, perpetual, royalty-free license (or license on such other terms that have been agreed by the Purchaser) for the Purchaser and/or the Replacement Service Provider to use such assets (with a right of sub-license or assign on the same terms); or

9.5.2 failing which procure a suitable alternative to such assets and the Purchaser or the Replacement Service Provider shall bear the reasonable proven costs of procuring the same.

9.6 The Service Provider shall as soon as reasonably practicable assign or procure the novation to the Purchaser and/or the Replacement Service Provider of the Transferring Contracts. The Service Provider shall execute such documents and provide such other assistance as the Purchaser reasonably requires to effect this novation or assignation.

9.7 The Purchaser shall:

9.7.1 accept assignations from the Service Provider or join with the Service Provider in procuring a novation of each Transferring Contract; and

9.7.2 once a Transferring Contract is novated or assigned to the Purchaser and/or the Replacement Service Provider, carry out, perform and discharge all the obligations and liabilities created by or arising under that Transferring Contract and exercise its rights arising under that Transferring Contract, or as applicable, procure that the Replacement Service Provider does the same.

9.8 The Service Provider shall hold any Transferring Contracts on trust for the Purchaser until such time as the transfer of the relevant Transferring Contract to the Purchaser and/or the Replacement Service Provider has been effected.

9.9 The Service Provider shall indemnify the Purchaser (and/or the Replacement Service Provider, as applicable) against each loss, liability and cost arising out of any claims made by a counterparty to a Transferring Contract which is assigned or novated to the Purchaser (and/or Replacement Service Provider) pursuant to paragraph 9.6 of this Schedule in relation to any matters arising prior to the date of assignation or novation of such Transferring Contract.

10. **SERVICE PROVIDER PERSONNEL**

10.1 The Service Provider shall not take any step (expressly or implicitly and directly or indirectly by itself or through any other person) to dissuade or discourage any employees engaged in the provision of the Services from transferring their employment to the Purchaser and/or the Replacement Service Provider.

10.2 During the Termination Assistance Period, the Service Provider shall give the Purchaser and/or the Replacement Service Provider reasonable access to the Service Provider 's personnel to present the case for transferring their employment to the Purchaser and/or the Replacement Service Provider.

10.3 The Service Provider shall immediately notify the Purchaser or, at the direction of the Purchaser, the Replacement Service Provider of any period of notice given by the Service Provider or received from any person referred to in the information to be provided by the Service Provider pursuant to Section D (staff involved in the provision of services) of the Contract, regardless of when such notice takes effect.

10.4 The Service Provider shall not for a period of twelve (12) months from the date of transfer actively seek to re-employ or re-engage or entice any employees, or Sub-Contarctors whose employment or engagement is transferred to the Purchaser and/or the Replacement Service Provider.

11. **CHARGES**

11.1 Except as otherwise expressly specified in this Contract, the Service Provider shall not make any charges for the services provided by the Service Provider pursuant to, and the Purchaser shall not be obliged to pay for costs incurred by the Service Provider in relation to its compliance with, this Schedule including the preparation and implementation of the Exit Plan, the Termination

Assistance and any activities mutually agreed between the Parties to carry on after the expiry of the Termination Assistance Period.

12. **APPORTIONMENTS**

12.1 All outgoings and expenses (including any remuneration due) and all rents, royalties and other periodical payments receivable in respect of the Transferring Assets and Transferring Contracts shall be apportioned between the Purchaser and the Service Provider and/or the Replacement Service Provider and the Service Provider (as applicable) as follows:

12.1.1 the amounts shall be annualised and divided by 365 to reach a daily rate;

12.1.2 the Purchaser shall be responsible for (or shall procure that the Replacement Service Provider shall be responsible for) or entitled to (as the case may be) that part of the value of the invoice pro rata to the number of complete days following the transfer, multiplied by the daily rate; and

12.1.3 the Service Provider shall be responsible for or entitled to (as the case may be) the rest of the invoice.

12.2 Each Party shall pay (and/or the Purchaser shall procure that the Replacement Service Provider shall pay) any monies due under paragraph 12.1 of this Schedule as soon as reasonably practicable.

This and the following single page comprise Schedule 11 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 11 - BUSINESS CONTINUITY AND DISASTER RECOVERY

1. SERVICE PROVIDER'S BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

The Service Providers Business Continuity and Disaster Recovery plan will be inserted following contract award.

This and the following 4 pages comprise Schedule 12 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 12 - SECURITY

DEFINITIONS

1.1 In this Schedule 12, the following definitions shall apply:

"**Breach of Security**" means the occurrence of:

(a) any unauthorised access to or use of the Services, the Sites, the Service Provider System and/or any ICT, information or data (including the Purchaser Protected Information, the Service Provider Sensitive Information, the Purchaser Data, and Customer personal data) used by the Purchaser and/or the Service Provider in connection with the Contract; and/or

(b) the loss and/or unauthorised disclosure of any information or data (including the Purchaser Protected Information, the Service Provider Sensitive Information, the Purchaser Data, and Customer personal data), including any copies of such information or data, used by the Purchaser and/or the Service Provider in connection with the Contract, in either case as more particularly set out in the Security requirements in this Schedule 12 and any relevant Security Policy;

(c) an unauthorised change to the integrity or accuracy of the information or data being processed.

2. **SECURITY MANAGEMENT PLAN**

2.1. Within twenty (20) Working Days after the Effective Date, the Service Provider shall prepare and submit to the Purchaser for Approval in accordance with paragraph 2 of this Schedule a fully developed, complete and up-to-date Security Management plan which shall comply with the requirements of paragraph 2.2 of this Schedule (the "**Security Management Plan**").

2.2. The Security Management Plan shall:

2.2.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan) to this Schedule12;

2.2.2 comply with the relevant security policies, and/or any security measures specified in Schedule 9 (Model Contract regarding Data Protection Directive 95/46/EC), and any other security policies and/or security measure notified to the Service Provider;

2.2.3 unless otherwise specified by the Purchaser in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Purchaser's premises, the Sites, the Service Provider System and any ICT, information and data (including the Purchaser Protected Information, the Service Provider Sensitive Information, the Purchaser Data, and Customer personal data) to the extent used by the Purchaser or the Service Provider in connection with the Contract;

2.2.4 set out the security measures to be implemented and maintained by the Service Provider in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule 12.

2.2.5 set out the plans for transiting all security arrangements and responsibilities from those in place at the Effective Date to those set out in the Implementation Plan for the Service Provider to meet the full obligations of the security requirements set out in Schedule Annex 1 (Security) to this Schedule 12.

2.2.6 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

2.2.7 be written in plain English in language which is readily comprehensible to the staff of the Service Provider and the Purchaser engaged in the Services and shall reference only documents which are in the possession of the Purchaser or whose location is otherwise specified in this Schedule 12.

2.3. If the Security Management Plan submitted to the Purchaser pursuant to paragraph 2.1 of this Schedule is Approved by the Purchaser, it shall be adopted by the Service Provider immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Purchaser, the Service Provider shall amend it within ten (10) Working Days of a notice of non-approval from the Purchaser and re-submit it to the Purchaser for Approval. The Parties shall use all reasonable endeavours to ensure that the Purchaser process takes as little time as possible and in any event no longer than fifteen (15) Working Days (or such other period as the Parties may agree in writing) from the date of the first submission to the Purchaser of the Security Management Plan. If the Purchaser does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Management Arrangements. No Approval to be given by the Purchaser pursuant to this paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in paragraph 2.2 of this Schedule shall be deemed to be reasonable.

2.4. Approval by the Purchaser of the Security Management Plan pursuant to paragraph 2.3 of this Schedule or of any change or amendment to the Security Management Plan shall not relieve the Service Provider of its obligations under this Schedule or the Contract.

3. **AMENDMENT AND REVISION OF THE SECURITY MANAGEMENT PLAN**

3.1. The Security Management Plan shall be fully reviewed and updated by the Service Provider from time to time and at least annually to reflect:

3.1.1. emerging changes in Good Industry Practice;

3.1.2. any change or proposed change to the Service Provider System, the Services and/or associated processes;

3.1.3. any new perceived or changed security threats; and

3.1.4. any reasonable request by the Purchaser.

3.2. The Service Provider shall provide the Purchaser with the results of such reviews as soon as reasonably practicable after their completion and the Security Management Plan at no additional cost to the Purchaser. The results of the review shall include, without limitation:

3.2.1. suggested improvements to the effectiveness;

3.2.2. updates to the risk assessments;

3.2.3. proposed modifications to the procedures and controls that effect information security to respond to events; and

3.2.4. suggested improvements in measuring the effectiveness of controls.

3.3. Subject to paragraph 3.4 of this Schedule, any change or amendment which the Service Provider proposes to make to the Security Management Plan (as a result of a review carried out pursuant to paragraph 3.1 of this Schedule, a Purchaser request, change to Annex 1 (Security) to this Schedule 12 or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until Approved in writing by the Purchaser.

3.4. The Purchaser may, where it is reasonable to do so, Approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to such procedures for the purposes of formalising and documenting the relevant change or amendment for the purposes of the Contract.

4. **BREACH OF SECURITY**

4.1. Either Party shall notify the other in accordance with the agreed security incident management process as defined by the Security Management Plan upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

4.2. Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 4.1 of this Schedule, the Service Provider shall:

4.2.1 immediately take all steps (which shall include any action or changes required by the Purchaser) necessary to:

(a) remedy such Breach of Security or any potential or attempted Breach of Security or protect the integrity of the Security Management Plan against any such Breach of Security or any potential or attempted Breach of Security; and

(b) prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

4.2.2 promptly provide to the Purchaser full details of the Breach of Security or the potential or attempted Breach of Security, including a root cause analysis where required by the Purchaser.

4.3. In the event that such action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance with any security policies notified to the Service Provider, the terms of the Security Management Plan, or security requirements or other requirements set out in the Contract (including this Schedule), or is otherwise due to the Default of the Service Provider, then any required change to the Security Management Plan shall be at no cost to the Authority.

5. PENETRATION TEST OF RELATED SYSTEMS

5.1. The Service Provider shall ensure that the Service Provider System is tested on at least an annual basis by an accredited tester and that vulnerabilities are actioned in line with recommended actions.

5.2. The Service Provider shall ensure that an accredited penetration test specific to the hosted website(s) is conducted: (i) on at least an annual basis; and (ii) promptly at any time during the Contract Period should significant changes be implemented that have the possibility of introducing weaknesses to those systems.

5.3. The Service Provider shall ensure that any recommended actions coming out of any testing outlined in paragraphs 5.1 and 5.2 are implemented promptly to remove or mitigate any discovered vulnerabilities.

5.4. The Service Provider will ensure that all checks and testing are aligned with business objectives (i.e. scope, constraints, deliverables) and that remedial actions are actioned promptly in line with business requirements.

ANNEX 1: SECURITY REQUIREMENTS

[NOTE: SECURITY REQUIREMENTS TO BE INSERTED FOLLOWING CONTRACT AWARD DEPENDING ON DATA TRANSFER REQUIREMENTS AND DETAILS BEING FINALISED.]

ANNEX 2: SECURITY MANAGEMENT PLAN

A Security Plan to be provided by Service Provider within 20 working days of Contract Award.

This and the following single page comprise Schedule 13 to the foregoing Contract between the Scottish Ministers and PeoplePlus Group Limited

SCHEDULE 13 - IMPLEMENTATION PLAN

1. SERVICE PROVIDER'S IMPLEMENTATION PLAN

An Implementation Plan to be provided by Service Provider within 10 Working Days of Contract Award.

Scottish Procurement and Commercial Directorate
Collaborative and Scottish Government Procurement Division

[redacted] gov.scot

PeoplePlus Group Limited
Blades Enterprise Centre
John Street
Sheffield
S2 4SW

Our Reference: Case/383612

Attn: [redacted]

18th October 2017

Dear [redacted]

Fair Start Scotland Employability Support Services 2018 Lot 8 Highlands

Following Scottish Government's previous letter of 22 September 2017, informing you of your success in the above competition, I now attached an annex which includes the electronic version of the contract documents which include the Entire Agreement Terms and Conditions, Annex I to Schedule 1: Technical Response and Annex J to Schedule 1: Clarifications.

Hard copies of the contract documentation will be provided at the Inception Meeting on 1st November 2017, further details will be provided under separate cover. You will be required at the meeting to sign and date two copies at page 46. This will constitute your formal acceptance of the binding Contract detailed therein.

With reference to Schedule 9 - Model Contract Regarding Data Protection Directive 95/46/EC, PeoplePlus Group Limited and Scottish Government representatives require to sign the Schedule at a forthcoming inception meeting. PeoplePlus Group Limited are responsible for completing "(the "Processor")" details prior to formal signature. A copy of the original signed document will be retained by Scottish Government and a copy held by PeoplePlus Group Limited.

The Contract shall commence on the "Effective Date" the date which this Contract is signed by both Parties. (October 2017) and end on 2 April 2021 with an option to extended up to 4 April 2023 (2 x 1 year options) or as otherwise terminated in accordance with the provisions of the Terms and Conditions of Contract.

Should you have any queries in relation to this letter, please contact me

Yours sincerely

[redacted]

[redacted]

Senior Portfolio Manager

Annex A

Entire Agreement (inc Terms and Conditions)

Fair Start Scotland - Lot 8 - PeoplePlus - Er

Annex I to Schedule 1: Technical Response

Fair Start Scotland - Lot 8 - PeoplePlus - A

Annex J to Schedule 1: Clarifications

Fair Start Scotland - Lot 8 - PeoplePlus - Ar

Annex J to Schedule 1 – Clarifications

i). Copy of Scottish Government correspondence dated 5th July 2017

Scottish Procurement and Commercial Directorate
Collaborative and Scottish Government Procurement Division

[redacted] gov.scot

The Scottish Government
Riaghaltas na h-Alba

All Tenderers

Our ref: SP-17-005

5 July 2017

Dear Sir,

WITHOUT PREJUDICE

Tender Reference: SP-17-005 - Invitation to Tender for Fair Start Scotland Employability Support Services 2018

Reference:

a. Tenderer's tender response of 24th May 2017
b. SP-17-005 dated 9th March 2017

As part of the tender evaluation process in relation to your company's tender response of the 24 May 2017 for the above mentioned requirement, Scottish Government has undertaken an initial review of your tender response and requests you to provide a response to the following information, as detailed:

As a part of this evaluation we have identified a small number of tenders where the Minimum Performance Expectations (MPE) requirements appear to have been misinterpreted by some tenderers.

The purpose of this clarification is two-fold. The first is to ensure complete transparency and common understanding on the MPE requirements for this service.

The second is to offer all tenderers the opportunity to revisit and resubmit their tender Technical response to any sections of the tender impacted by this clarification**.** The word limit set out in the ITT applies as before to each question. Please also provide a short covering note setting out why and how this clarification has impacted on your offer.

Where any resubmission results in a change to the number of outcomes being offered, these numbers will be transferred to your pricing proposals to recalculate the price per outcome. This will in turn impact on the baseline cost calculation.

Minimum Performance Expectations.

As set out in Paragraph 21.11 of the Fair start Scotland Specification, the Minimum Performance Expectations in respect of the Key Performance Indicators at a Strand Level are:

Service Strand	13 week Job Outcomes (% of starts on the Programme)	26 weeks Sustained Job Outcome (% of 13 week Job Outcomes)	52 weeks Sustained Job Outcome (% of 13 week Job Outcomes)
Core Strand	41%	84%	70%
Advanced Strand	27%	84%	70%
Intense Strand	28%	84%	70%

Annex D to Schedule 1 sets out how these percentages translated into anticipated volumes for each lot. Please see example below using Glasgow's figures.

Strand	13 Week Job Outcome	26 Week Sustain % of 13 Week JO	26 week Sustain	52 week sustain % of 13 week JO	52 week sustain
Core	**436**	84%	366	70%	305
Advanced	**1026**	84%	862	70%	718
Intense	**766**	84%	644	70%	536
Total	2228	84%	1872	70%	1560

For the avoidance of doubt, whether a tenderer offers more 13 week outcomes than the minimum number or just the minimum for that strand and lot then the 26 week

and 52 week sustainment's must represent at least **84%** and **70%** respectively of the number of 13 week job outcomes in your offer.

For example, in the lot above, if your offer for core job outcomes is 450, then the 26 week outcomes must be at least 378 (84%) and 315 (70%) for 52 week sustainment's.

If your offer falls below these percentages for any of the strands it will be scored as "0" regardless of the rationale provided as it fails to meet our minimum requirements and will be considered non-compliant for the purpose of the Fair Start Scotland competitions.

Where your offer does meet or exceed MPE as described above it will be scored on the basis of the rationale provided.

Tenderers are requested to review the clarification request and provide a response, and complete the attached Form of Tender, through the dedicated PCS-T messaging area by **1200 hrs** on **12 July 2017**. No other form of communication will be accepted and no queries or questions will be answered by the Authority after the period of the deadline has elapsed.

Please note that this letter must not be taken to imply that your offer is acceptable and is written without prejudice to the terms and conditions of the Invitation to Tender document.

In the meantime if you require to discuss further, please contact me via PSCT.

Yours sincerely

[redacted]

Senior Portfolio Specialist

ii). Copy of PeoplePlus Group Ltd PCS-T response dated 11th July 2017

Sent from Use [redacted]

Good Afternoon

We have noted the content of the **Scottish** Government's letter of 5th July 2017 and our original tender submission of 24th May 2017 remains valid.

We believe our response for the Glasgow Lot and the Highlands and Islands Lot are correct and above the Minimum performance expectation.

Kind Regards

iii). Copy of Scottish Government correspondence dated 11th August 2017

Scottish Procurement and Commercial Directorate
Collaborative and Scottish Government Procurement Division

[redacted].scot

The Scottish Government
Riaghaltas na h-Alba

PeoplePlus Group Ltd
By Email: Via Public Contracts Scotland Tender
(e-tender Portal)

Our ref: SP-17-005

Date: 11th August 2017

Dear Sir/Madam,

WITHOUT COMMITMENT

Tender Reference: SP-17-005
Invitation to Tender for Fair Start Scotland Employability Support Services 2018

As part of the tender evaluation process in relation to your company's tender of the 23rd May 2017 for the above mentioned requirement, we have undertaken an initial review of your tender response and require clarification from you in respect of the following:

Lot 8 – Highlands

ESPD (European Single Procurement Document)

Sub-contractors Part 2 - General Information

Q 2A.14

Please confirm the size of the listed Sub-contractor organisations based on the definition of a small or medium enterprise:

- LifeSkills
- Lochaber Hope
- 2020 Clearview

Part 3D – Misrepresentation

Q.3D.15.1

Please confirm that Argyll & Bute Council has not been guilty of serious misrepresentation in supplying the information required for the verification of the absence of grounds for exclusion or the fulfilment of the selection criteria?
3D.15.2

Please confirm that Argyll & Bute Council has not withheld such information referred to in Q 3D.15.1?

3D.15.4

Please confirm that Argyll & Bute Council has not undertaken to unduly influence the decision making process of the organisation or contracting entity, to obtain confidential information that may confer upon it undue advantages in the procurement procedure or to negligently provide misleading information that may have a material influence on decisions concerning exclusion, selection or award?

Commercial – Pricing Schedule

Lot 1 - Glasgow and Lot 8 - Highland

Contingency Costs

Scottish Government requests PeoplePlus to provide a breakdown of their assumptions underpinning their proposed contingency costs of [redacted] (Lot 1) and [redacted] (Lot 8) for undertaking clerical activity.

Please advise the components of the proposed cost(s) and the period of time that you have assumed the contingency arrangements, if required, would be in place for.

Finally, please clarify how these costs would be affected if the actual period of contingency was different from that assumption.

Breakdown of Costs

Management Fee (if any) in payments to delivery partners/supply chain/ consortia members.

For the avoidance of doubt Scottish Government request PeoplePlus to explain the Management Fee entry which shows a negative figure of: - [redacted] (Lot 1) and - [redacted] (Lot 8) and confirm how much you are charging as a management fee.

Customer Costs

For the avoidance of doubt Scottish Government request PeoplePlus to confirm that no customer costs are applicable for the Intense Strand (Lot 1) or that these costs are covered within: 'Payments to delivery partners/supply chain/ consortia members'. Please confirm if a similar arrangement may apply to Lot 8 for all 3 strands.

Technical

Lot 1 - Glasgow and Lot 8 - Highland

Q.1.1.3 – Customer Journey Stages

PeoplePlus are required to confirm the frequency of 'face to face' engagement with customers since Scottish Government, as detailed within the Specification (Schedule 1) requires this to be undertaken weekly and it is not clear from the response if this is your intention.

Please confirm whether the diagnostic tools mentioned within Stage 6 – Weeks 1 to 3 will be adopted by all Supply Chain Partners.

Your tender response states "PeoplePlus has unique access to 75 national employers across Scotland". Please confirm how many employers will be engaged in the delivery of the service actually within Lot 1 and Lot 8 respectively.

Lot 8

Q.1.1.4 – Customer Journey – Service Strand

Your response includes a reference to Jobcentre Plus as a Specialist Support Provider. Please clarify the role of JobcentrePlus in the delivery of the FSS service.

Lot 8

Q.1.1.5 - Delivery Mechanism

Please clarify who will be responsible for delivering each stage of the Customer journey in each of the Local Authority areas within the Lot.

Lot 8

Q.1.1.9 - Delivery Locations

The Fair Start Scotland Specification (paragraph 5.8) states that the Scottish Government requires minimum core hours for the Service to be 09.00 to 17.00. Your tender states "…. We will have flexible opening hours." Please clarify what is meant by flexible opening hours. Please confirm that you will adhere to the minimum core hours for the Service?

Please clarify what support will be available to Customers who cannot access your 'MyTime' mobile phone App.

Please confirm that Jobcentre Plus are agreeable to using their premises deliver the FSS service.

Lot 8

Q.1.1.15 - Employer Engagement

Please confirm who will employ the Employer Relationships Managers and who will be responsible for managing the Employer Relationships Managers.

Lot 1

Q.1.2.1 – Management Structure

Scottish Government note that Performance development reviews are undertaken every 6 months with Suppliers and request PeoplePlus to clarify what are their procedures for improving/reviewing performance during the interim period.

Lot 8

Q.1.2.1 – Management Structure

Please clarify the relationship between PeoplePlus, your Delivery Partners and the Specialist Delivery Partners.

Lot 8

Q.1.4.1 – Communications and Marketing (Customers)

Your tender proposes to market the service through a range of marketing material and literature and mentions "GP surgeries (intense strand)". The Service Specification (para 7.5) states that Service Providers must refrain from using the Service Strand terminology or jargon. Please confirm that all marketing material and literature will not make any references to the Core, Advanced and Intense Service Strands.

Q.1.4.2 – Communications and Marketing (Referral Agencies)

Your tender proposes to agree "local level target and maximum monthly referral numbers with key referring agencies against the three service strands. The Scottish Government do not consider referral targets for individual Referral Agencies are appropriate for this Service. Please confirm that this element of your proposal will be withdrawn.

Your tender proposes "to co-locate with key RAs (e.g. weekly, dependent on referral volumes), to accept referrals directly … ". Please clarify the arrangements proposed for co-location.

Lot 1

Q.1.5.4 – Risk Management

PeoplePlus are requested to consider the extent to which quarterly review of risk affects their ability to inform Scottish Government immediately of any risks which materialise which may have an impact on the operation of contract.

Lot 1 & 8

Q.1.5.7 – Security

You are requested to clarify what process they follow when decommissioning PCs, laptops and servers to ensure that there is no recoverable information on the storage media of these devices?

Where you have provided an identical or near identical response for any one Lot please confirm that you intend the clarification to be carried over to all subsequent Lots. For example if we ask you to clarify Question 1.1.3 – Customer Journey Stages in one Lot, please confirm that you wish the clarification response to apply to subsequent Lots for which you submitted a tender. Where you do not confirm this, we will assume the clarification response is Lot specific and refers only to the Lot for which the question has been raised.

Please note that the clarification process does not offer you the opportunity to augment or make any changes to your tender. The purpose is to **clarify** areas of your tender where there may have been ambiguity or where further clarity may be required. Tenders will not be rescored or re-evaluated in light of any clarification responses, scores attributed to your tender will stand.

This letter must not be taken to imply that your offer is acceptable and is written without prejudice to the terms and conditions of the Invitation to Tender document.

Please submit your response to arrive not later than midday on 18th August 2017.

Yours faithfully

[redacted]

[redacted]

Senior Portfolio Manager

iv). PeoplePlus Group Ltd correspondence dated 14th August 2017

Tender Ref: SP-17-005

Date: 14th August 2017

Dear [redacted]

Please find below our response to the clarification questions raised for the following:
Invitation to Tender for Fair Start Scotland Employability Support Services 2018 – Lot 1 Glasgow and Lot 8 Highlands:

Lot 8 – Highlands

ESPD (European Single Procurement Document)

Sub-contractors Part 2 - General Information

Q 2A.14

Please confirm the size of the listed Sub-contractor organisations based on the definition of a small or medium enterprise:

- LifeSkills
- Lochaber Hope
- 2020 Clearview

Response: *We can confirm for Lot 8, the size of our listed sub contractors are as follows:*

- LifeSkills - *SME (Medium, between 50 and 250 staff)*
- Lochaber Hope – *SME (Small, fewer than 50 staff)*
- 2020 Clearview – *SME (Small fewer than 50 staff)*

Part 3D – Misrepresentation

Q.3D.15.1

Please confirm that Argyll & Bute Council has not been guilty of serious misrepresentation in supplying the information required for the verification of the absence of grounds for exclusion or the fulfilment of the selection criteria?

Response: *We can confirm that Argyll & Bute Council has confirmed that they have not been guilty of serious misrepresentation in supplying the information required for the verification of the absence of grounds for exclusion or the fulfilment of the selection criteria.*

3D.15.2

Please confirm that Argyll & Bute Council has not withheld such information referred to in Q 3D.15.1?

Response: *We can confirm that Argyll & Bute Council has confirmed that they have not withheld such information referred to in Q 3D.15.1.*

3D.15.4

Please confirm that Argyll & Bute Council has not undertaken to unduly influence the decision making process of the organisation or contracting entity, to obtain confidential information that may confer upon it undue advantages in the procurement procedure or to negligently provide misleading information that may have a material influence on decisions concerning exclusion, selection or award?

Response: *We can confirm that Argyll & Bute Council has confirmed that they have not undertaken to unduly influence the decision making process of the organisation or contracting entity, to obtain confidential information that may confer upon it undue advantages in the procurement procedure or to negligently provide misleading information that may have a material influence on decisions concerning exclusion, selection or award.*

Commercial – Pricing Schedule

Lot 1 - Glasgow and Lot 8 - Highland

Contingency Costs

Scottish Government requests PeoplePlus to provide a breakdown of their assumptions underpinning their proposed contingency costs of [redacted] (Lot 1) and [redacted] (Lot 8) for undertaking clerical activity.

Please advise the components of the proposed cost(s) and the period of time that you have assumed the contingency arrangements, if required, would be in place for.

Finally, please clarify how these costs would be affected if the actual period of contingency was different from that assumption.

Response:

- *In Lot 1, PeoplePlus has assumed 1 FTE over the full 4.25 years of the contract [redacted] plus [redacted] of JMS development costs.*

- *In Lot 8, PeoplePlus have assumed 0.32 FTE for the full 4.25 years of the contract [redacted] lus [redacted] of JMS development costs.*

If the actual period of contingency was different to the assumption, this would directly impact the staffing requirement across both Lots. Staffing would be required on an annual basis as follows:

- *Lot 1: [redacted] per year*
- *Lot 8: [redacted] per year*

Lots 1 & 8: The [redacted] of JMS development costs (if required) is a fixed fee therefore will remain the same cost regardless of the actual period of contingency.

Breakdown of Costs

Management Fee (if any) in payments to delivery partners/supply chain/ consortia members.

For the avoidance of doubt Scottish Government request PeoplePlus to explain the Management Fee entry which shows a negative figure of: - [redacted] (Lot 1) and - [redacted] Lot 8) and confirm how much you are charging as a management fee.

Response: *Lots 1 & 8: The management fee is included as a negative figure as the 'Payments to Delivery partners/supply chain/consortia members' is the gross amount of the contract value payable to our partners. PeoplePlus will then take a management fee from the Delivery Partners equivalent to [redacted] of this gross payment. The [redacted] Management fee includes:*

- ***Specialist Self-employment Provision*** *– PeoplePlus are a leading provider of self employment provision in Scotland and expect circa 10% of all outcomes across each strand to come via the self-employment route. PeoplePlus will provide Specialist Self-employment provision across all 3 strands on behalf of our delivery partners. This has been agreed as part of the Management Fee with our partners, which will yield better results for partners and customers alike. This includes:*
    - *Specialist Business Advisors (Lot 1 – 3 FTE and Lot 8 – 1 FTE)*
    - *The Enterprise Portal – providing a wealth of self-employment resources, videos, how to guides and Podcasts*
    - *Enterprise App – where customers can learn more about self-employment*
    - *Access to existing networks and referrals agencies across Scotland via PeoplePlus existing national NEA contract, including Business Gateway relationships and sub contractor cross referral networks*
    - *Enterprise Management time and expertise*
    - *Access to 100 Enterprise experts nationally plus Mentors*
    - *Specialist training for Enterprise staff, sector specific.*

- ***Supply Chain Management –*** *The supply chain management fee will also include costs for the following:*
    - *Integration Manager (LOT 1 – 1 FTE and LOT 8 - 0.5 FTE)*
    - *Use of JMS and License Fees*
    - *Use of PeoplePlus Diagnostic Assessment Tools & relevant training*
    - *PeoplePlus Policies and Processes*
    - *Commercial support and contract guidance/interpretation*
    - *Bespoke SharePoint Site access including a variety of resources and information including Industry updates and teaching materials, equality and diversity and safeguarding materials*
    - *Staff development and training (includes Safeguarding, Prevent Duty and embedding British Values, Observation skills, teaching and learning CPD and Equality and Diversity)*
    - *Environmental and Sustainability support and information (includes Carbon footprint tools)*
    - *External Audit and Assessment Support in preparation for funder and Accreditation organisation visits*
    - *Business Support & Financial Claims Support, including guidance updates and Live Running memos*

- *Management Information Reports & bespoke customer data exports*
- *Customer Journey Development and troubleshooting project support*
- *Supply Chain Partner meetings for sharing best practice and reviewing contract performance*
- *Access to PeoplePlus, Staffline (including Bright Works) job opportunities*
- *Contract Assurance Officer function to check for quality and compliance of learner/customer records*
- *Financial planning and modelling tools*
- *Continuous Quality Improvement support through quality reviews and due diligence checks*
- *Customer feedback tools and reporting, including support and advice to help deal with customer complaints*
- *Advice and support with safeguarding controls and managing concerns*
- *Health, Safety and Security support and advice*
- *Subject matter experts to review partner policies and procedures and offer feedback and guidance*
- *Subject matter experts are available to support in the resolution of any potential Safeguarding/E&D/Prevent (Anti-Radicalisation) incidents*
- *Support in reporting and controlling Information Security incidents and associated queries*

Customer Costs

For the avoidance of doubt Scottish Government request PeoplePlus to confirm that no customer costs are applicable for the Intense Strand (Lot 1) or that these costs are covered within: 'Payments to delivery partners/supply chain/ consortia members'. Please confirm if a similar arrangement may apply to Lot 8 for all 3 strands.

Response: *For Lot 1 Intense Strand and for Lot 8 all strands the customer costs will be covered by the Delivery Partners/Supply Chain out of their payment highlighted in the Pricing Schedule. For Lot 8 the Payment to the Delivery Partners would be a gross amount of [redacted] less the management fee of [redacted]. So a net payment of [redacted] will be made from he customer costs will be covered*.

Technical

Lot 1 - Glasgow and Lot 8 - Highland

Q.1.1.3 – Customer Journey Stages

PeoplePlus are required to confirm the frequency of 'face to face' engagement with customers since Scottish Government, as detailed within the Specification (Schedule 1) requires this to be undertaken weekly and it is not clear from the response if this is your intention.

Response: *PeoplePlus can confirm that in Lots 1 & 8, the frequency of 'face to face' engagement with customers is undertaken weekly in line with the specification*.

Please confirm whether the diagnostic tools mentioned within Stage 6 – Weeks 1 to 3 will be adopted by all Supply Chain Partners.

Response: *PeoplePlus can confirm for Lots 1 & 8 that the diagnostic tools mentioned within stage 6 – Weeks 1 to 3 will be adopted by all Supply Chain Partners.*

Your tender response states "PeoplePlus has unique access to 75 national employers across Scotland". Please confirm how many employers will be engaged in the delivery of the service actually within Lot 1 and Lot 8 respectively.

Response: *PeoplePlus can confirm that of the 75 national employers, 51 will be specifically engaged in the delivery for Lot 1 and 23 in Lot 8. In addition, across both lots PeoplePlus and our supply chain have access to a significant amount of local employers in each Lot, which is also supplemented via our local Staffline and Brightworks Accounts, for example across the Highlands and Islands our Supply Chain network current works directly with in excess of 150 local Employers.*

Lot 8

Q.1.1.4 – Customer Journey – Service Strand

Your response includes a reference to Jobcentre Plus as a Specialist Support Provider. Please clarify the role of JobcentrePlus in the delivery of the FSS service.

Response: *For Lot 8, we can confirm that Jobcentre Plus has been listed in error and will not be a Specialist Support Provider*.

Lot 8

Q.1.1.5 - Delivery Mechanism

Please clarify who will be responsible for delivering each stage of the Customer journey in each of the Local Authority areas within the Lot.

Response: *Please see below table outlining who will be responsible for delivering each stage of the Customer Journey in each of the Local Authority Areas in Lot 8:*

Local Authority	Core Strand	Advanced Stand	Intense Strand
Argyll & Bute	*Argyll & Bute Council*	*Argyll & Bute Council*	*Argyll & Bute Council*
Eilean Siar	*3rd Sector Hebrides*	*3rd Sector Hebrides*	*3rd Sector Hebrides*
*Highland**	*Lifeskills** *LochAber Hope** *2020 Clearview **	*Lifeskills** *LochAber Hope** *2020 Clearview**	*Momentum** *LochAber Hope** *2020 Clearview**
Moray	*Lifeskills*	*Lifeskills*	*Momentum*
Orkney Islands	*Lifeskills*	*Lifeskills*	*Lifeskills*
Shetland Islands	*Lifeskills*	*Lifeskills*	*Lifeskills*

** Lifeskills will deliver across Dingwall, Invergordon & Inverness and surrounding areas*
** LochAber Hope will deliver across Fort William & Portree and surrounding areas*
** 2020 Clearview will deliver across Wick & Thurso and surrounding areas*
** Momentum will deliver across Dingwall, Invergordon & Inverness and surrounding areas*

Lot 8

Q.1.1.9 - Delivery Locations

The Fair Start Scotland Specification (paragraph 5.8) states that the Scottish Government requires minimum core hours for the Service to be 09.00 to 17.00. Your tender states "…. We will have flexible opening hours." Please clarify what is meant by flexible opening hours. Please confirm that you will adhere to the minimum core hours for the Service?

Response: *We can confirm that we will adhere to the minimum core hours for this service i.e. 09.00 to 17.00. Our flexible opening hours mean that staff are able to support customers outside of the minimum core hours for the service, this could be for example an 8.00am call to ensure that a customer is up and prepared for their interview at 10.00am or in-work support available after 5.00pm for customers working shift patterns. This is applicable to Lot 1 & Lot 8.*

Please clarify what support will be available to Customers who cannot access your 'MyTime' mobile phone App.

Response: *MyTime is available via an App or via the web. For customers not able to access the MyTime App they are able to access the same content via a web platform. Customers that do not have access to the internet and/or IT equipment can access this by visiting one of our centres where MyTime will be available on a range of PCs and basic IT training will be available to all customers to enable them to access and utilise the MyTime platform. Customers with a learning difficulty/disability are able to receive face to face/telephone support relevant to their individual needs to ensure equality of access to MyTime, this may include the use of electronic or paper based versions where applicable. This response is applicable to Lot 1 & Lot 8.*

Please confirm that Jobcentre Plus are agreeable to using their premises deliver the FSS service.

Response: *In Lot 8, all of our partners currently operate in Highlands and Islands with good and extensive relationships with JCP's, with existing co-location agreements in place which will be utilised going forward if we are successful with Fair Start. Please see below for additional quotes from some of our partners:*

Momentum - *We have strong relationships with a number of JCP sites across the highlands and islands (from Oban to Shetland) where we currently have access to onsite resources such as 1:1 rooms or desks where we can support our existing WFS customers (these are relationships which have continued following the end of WC with no challenge). We are yet to work with a JCP site which has been unable to accommodate our advisors*.

LochAberHope- *We have a very good relationship with JCPs in Highland and currently have an agreement in place to use their premises in delivering current programme. JCP are agreeable for us to use the premises to deliver partner programmes.*

2020Clearview - *The Job Centre in Caithness and Sutherland is located in Wick. We have a very close working relationship with this office and are lucky enough to enjoy an "open door" policy in terms of us accessing Job Centre front line staff, advisors and management. This is crucial when working in this remote rural area where there are huge difficulties with transport and communication. We have an agreement that we can use the local Wick Job Centre premises as and when required for a range of activities including initial assessments, interviews, presentations, information sessions, group training sessions etc. We currently*

have weekly caseload meetings with Work Coaches to discuss provision, any issues, forthcoming plans, etc and this effective joint working means we will continue to deliver the most effective provision for our customer.

Third Sector Hebrides - *Third Sector Hebrides have a very close relationship with Stornoway Job Centre, we speak to each other on a daily basis and are located on the same street and have attended sessions at the Job Centre at their request, to promote Work Able to a selected cohort of customers and liaise regularly with Job Coaches to discuss client progress- I would expect a similar procedure with FSS.*

Argyll and Bute Local Authority - *Argyll and Bute Council have premises throughout the whole of our local authority area from which we currently deliver all contracts. In addition to this JCP have premises in Campbeltown, Oban, Dunoon, Rothesay and Helensburgh. We have an excellent relationship with all JCPs and if necessary we are able to meet customers in their premises.*

Lifeskills - *As a current delivery partner of most of the main programmes in the Highlands and Islands, Lifeskills have existing co-location agreements in place with JCP across the Highlands and Islands and work well with these partners on our current contract delivery , these agreements will continue to be in place should we be successful with fair start across this region.*

Lot 8

Q.1.1.15 - Employer Engagement

Please confirm who will employ the Employer Relationships Managers and who will be responsible for managing the Employer Relationships Managers.

Response: *In Lot 8, we can confirm that the Employer Relationship Managers will be employed by our Supply Chain partners and the Supply Chain partners will be responsible for managing the Employer Relationship Managers.*

Lot 1

Q.1.2.1 – Management Structure

Scottish Government note that Performance development reviews are undertaken every 6 months with Suppliers and request PeoplePlus to clarify what are their procedures for improving/reviewing performance during the interim period.

Response: *In-line with our Supply Chain Management Framework, we conduct a quarterly Performance Development Review with each supplier conducted by our Service Manager. Our procedure for improving/reviewing performance of suppliers during the interim period includes a monthly Partner Monitoring Review meeting to review Key Performance Indicators which include: Staff Resource – This covers, Staff CPD, Teaching and Learning Observations; Organisation Chart review and Recruitment Activity; Other KPIs reviewed include: Contractual Performance, Customer Service Continuity, Customer Satisfaction, Customer Complaints, Overall value for money, Equality and Diversity and Sustainable Development. This applies to Lot 1 and Lot 8.*

Lot 8

Q.1.2.1 – Management Structure

Please clarify the relationship between PeoplePlus, your Delivery Partners and the Specialist Delivery Partners.

Response: *In Lot 8, PeoplePlus are the Prime Contractor/Managing Agent for the Fair Start Scotland Contract, our Delivery Partners are sub-contracted directly to PeoplePlus for the delivery of the relevant Fair Start Service Strand on an end to end basis. Our Specialist Delivery Partners are approved by PeoplePlus under our Supply Chain Management Framework for call-off services that will be contracted directly by our Delivery Partners. The performance and quality of all supply chain partners will be managed as per our Supply Chain Management Framework requirements, this includes the performance and quality of Specialist Delivery Partners which will be reviewed by our Delivery Partners on a monthly basis and reviewed quarterly by PeoplePlus*.

Lot 8

Q.1.4.1 – Communications and Marketing (Customers)

Your tender proposes to market the service through a range of marketing material and literature and mentions "GP surgeries (intense strand)". The Service Specification (para 7.5) states that Service Providers must refrain from using the Service Strand terminology or jargon. Please confirm that all marketing material and literature will not make any references to the Core, Advanced and Intense Service Strands.

Response: *We can confirm for both lot 1 & 8 that as per the Service Specification all marketing material and literature will not make any references to the Core, Advanced and Intense Service Strands.*

Q.1.4.2 – Communications and Marketing (Referral Agencies)

Your tender proposes to agree "local level target and maximum monthly referral numbers with key referring agencies against the three service strands. The Scottish Government do not consider referral targets for individual Referral Agencies are appropriate for this Service. Please confirm that this element of your proposal will be withdrawn.

Response: *We can confirm for both Lot 1 & 8 that this element of our proposal will be withdrawn.*

Your tender proposes "to co-locate with key RAs (e.g. weekly, dependent on referral volumes), to accept referrals directly … ". Please clarify the arrangements proposed for co-location.

Response: *In Lot 8, due to the rural and remote nature of working within the Highlands and Islands, our partners have a variety of co-location arrangements in place currently and all partners propose to continue with these arrangements for Fair Start. Co-location arrangements for each partner include:*

LochAberHope- *West Highland College, Criminal Justice Department, JCP's, Highland Council Employability, Voluntary Action Lochaber, Lochaber Action on Disability, Community Mental Health.*

Momentum- *Have an existing range of co-location agreements across the Highlands and Island and already work with many referral agencies for existing contracts such as Work Choice, so these already exist.*

2020Clearview - *Have built up a network of co-location agreements within their area and regularly work with organisations such as: The Highland Council - Employability, Housing, Finance & Social Services Departments; the NHS - Caithness & Sutherland Mental Health Units, Birchwood, Homelink, PPP Home Care; Barnardo's, The Shirlie Project, CAB, Lairg Learning Centre and Brora Learning Centre. The Highland Council will continue to use 2020 Clearview to deliver outreach employability support services to the vulnerable individuals who live throughout this remote and rural area. They are able to access Council premises, Community & Learning Centres etc in villages throughout the area in order to ensure no matter where a customer lives, they can access professional support and advice. They will also continue current arrangements with Citizen's Advice Bureaux in Wick, Thurso and Golspie.*

Argyll and Bute Local Authority – *have stated that they have no problem co-locating with referral agencies and currently work with: Skills Development Scotland; Jobcentre Plus; Capability Scotland; Argyll College UHI; Argyll Third Sector; Working Rite; NHS Health; Argyll and Bute Council. They also signpost and work with: Addaction (drug and alcohol issues), Argyll TSI (Third Sector Interface) for opportunities within voluntary sector; Community Learning and Development (relevant courses); DASH Recovery Café (mental health and drug and alcohol service); Link Club (mental health issues); Welfare Rights Service (money advice and benefits); Home Majik (health and wellbeing); KADAS (drugs and alcohol); OASIS (addiction); DOCHAS (counselling, bereavement support, etc); Young Carers Group.*

Lifeskills - *have a range of co-location agreements in place such is the nature of working within the Highlands and Island and already work with many referral agencies for existing contracts including: NHS, JCP, Deaf Action, SAMH, Citizen Advice Bureau and Chamber of Commerce.*

Lot 1

Q.1.5.4 – Risk Management

PeoplePlus are requested to consider the extent to which quarterly review of risk affects their ability to inform Scottish Government immediately of any risks which materialise which may have an impact on the operation of contract.

Response: *Our Audit and Risk Committee meet on a quarterly basis to review all divisional risk plans in line with our Risk Management Policy and Group Plc internal reporting process as set out by the Staffline Board. Each Risk Plan is a live document and is updated by the Risk Plan owner to reflect real time. Any risks or incidents that materialise that may have an impact on the operation of the contract are immediately reported to the Operational Director and the Governance Director who will inform the Scottish Government and activate Disaster Recovery protocols Immediately. This applies to both Lot 1 & Lot 8.*

Lot 1 & 8

Q.1.5.7 – Security

You are requested to clarify what process they follow when decommissioning PCs, laptops and servers to ensure that there is no recoverable information on the storage media of these devices?

1.1 Response: ***For Lot 1 & Lot 8, PeoplePlus is an ISO27001 accredited provider and have robust systems in place for the decommissioning of PC's, Laptops and servers, completed in-line with our approved DWP Security Plan, Security Policy; and our Disposal and Decommissioning Policy as outlined below:***

Document Destruction

All personal and corporate information processed manually using hard copy paper based records and files that are no longer required should be destroyed in line with contractual and legal obligations. The destruction method should ensure of all records are disposed of in a way which prevents republishing or further distributed. In PeoplePlus this is achieved by disposing of the material in a confidential waste bin which is emptied on a regular basis by a designated contractor. If a location does not have a confidential waste bin the material must be shredded. The minimum destruction requirement requires the shredding of paper based records using a cross cut shredder that cuts the paper into pieces of no more than 15mm x 4 mm.

If a location is closing or a shredder is not available paper based documents containing confidential information should be stored in a secure location usually the confidential waste bin or other secure location prior to being sent for destruction. PeoplePlus only uses approved contractors to collect and dispose of this confidential waste.

Electronic Data Destruction

All personal data must be stored in secure databases and/or systems or secured networks. All IT equipment must be disposed of via the IT department to ensure all confidential is removed and that hard disks are cleared of all software and all confidential information prior to disposal or re-use. The ICT Service Delivery Manager is responsible for the secure disposal of storage media and the disposal of all information processing equipment. All storage media will be disposed of in line with HMG Information Assurance Standard 5 – Secure Sanitisation guidelines. A log will be retained showing what media were destroyed, disposed of, and when. The asset inventory is adjusted once the asset has been disposed of.

Operational and Support Managers are responsible for notifying ICT of all equipment which requires de-commissioning and disposal. Staff outside of ICT Department are not authorised to destroy or dispose of IT equipment. This includes removable media such as CDs/DVDs, portable hard disks, USB data sticks, SD cards etc.

All equipment awaiting destruction will be stored in a secure area with limited access. A log will be kept of all equipment held in the secure area and such equipment will be subject to random audits.

Devices containing confidential information that are damaged will be subject to a risk assessment from the Head of Assurance to establish whether the device should be repaired or replaced.

Paper based documents containing confidential information will be stored in a secure location prior to being sent for destruction. The company will use approved contractors to collect and dispose of this confidential waste.

Hard disks from photocopying and printing devices will also be subject to secure disposal as per this policy.

Where machines are to be re-deployed internally they will be subject to a re-image using the company's standard build.

Machines issued to external parties such as subcontractors will either be issued as new devices or will have been subject to secure disk wiping using a CESG approved product before being deployed. Such machines remain the property of the company and subcontractors are not authorised to destroy or dispose of these machines.

Network devices such as firewalls, routers and switches will be de-commissioned by the ICT department and will be subject to a secure wiping procedure before disposal.

All equipment will be disposed of in line with Waste Electrical and Electronic Equipment (WEEE) directive. Copies of certificates for the destruction of such equipment will be retained by the ICT Service Delivery Manager.