EVALUATION OF THE TREE HEALTH PEST AND DISEASE SURVEYS SCOTLAND FRAMEWORK

FREEDOM OF INFORMATION REQUEST: 2020/00032394

Name	GDPR Statement
A & R Woodland Consultant	The EU General Data Protection Regulation (GDPR) is a privacy and data protection regulation in the European Union effective from May 25 2018. The GDPR imposes new obligations on organisations that control or process personal data and introduces new rights and protections for EU citizens. A & R Woodland Consultants Ltd are committed to ensuring that your privacy is protected and we strictly adhere to the provisions of all relevant Data Protection Legislation, including GDPR, ensuring all personal data is handled in line with the principles outlined in the regulation that state: Personal data shall be: 1. Processed lawfully, fairly and in a transparent manner in relation to the data subject 2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes 3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed 4. Accurate and, where necessary, kept up to date 5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed 6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures 7. Destroyed in a suitable and safe manner when data is no longer required A & R Woodland Consultants Ltd respect our customer rights to data privacy and protection and as such we have revised our internal policies, procedures, working practices in order to meet the requirements of the GDPR.

	A & R Woodland Consultants Ltd are committed to compliance with the GDPR as both a processor and controller of personal data. We place a high priority on protecting and managing data in accordance with accepted standards and indeed helping our customers utilise our products and services to the same end. All employees of A & R Woodland Consultants are aware of the GDPR and restrictions and obligations within it which are relevant to them. Suppliers and sub-contractors who may process personal details on behalf of A & R Woodland Consultants Ltd will be identified and asked to provide details on their state of compliance with the GDPR. Any new supplier or sub-contractor will not be taken on unless we are satisfied that they comply with the new data protection regulations.
Andy Stewart Forestry	We confirm that Andy Stewart Forestry and Estate Services Ltd will ensure that all data and information gathered as part of fulfilment of the tender will be stored, processed and destroyed in a manner that is compliant with the requirements of the GDPR.
JM Tree Works	Data and information will primarily be stored in paper copy within a locked office, only 2 key holders. Electronic data is stored on a standalone hard drive within the office, password protected and not networked. Data processing will only take place to meet Employment Obligations and to deliver the contract. A key third party will be Scottish Forestry, they will require copies of training and competency certificates, where practical able address details and other personal information (information not required to be provided) will be removed or blacked out. Employment and Financial records will be retained for 6 years and all other records for 2 years. Paper documents will be destroyed by shredding and for electronic records/information will be destroyed by permanent deletion and/or factory reset.
M H Cope Forestry Consultant	All data and information gathered in relation to the fulfilment of this tender will be stored, process and destroyed in a manner which is fully compliant with GDPR
Murray Forestry	Our Forestry manager has internal FC training regarding data protection and we have a policy in place to ensure we process, handle and dispose of data ensuring we are

	compliant with GDPR regulations. We have a permissions procedure in place for staff to ensure data handling is understood and in agreement with all, whilst sharing procedures are understood. **Privacy notice** • Murray Forestry Ltd requires its staff, directors and others who have access to Murray Forestry Ltd's information and communications facilities (eg temporary staff, consultants, etc) to comply with the principles of the Data Protection Act 1998 and the General Data Protection Regulation 2018 (GDPR) and maintain data confidentiality at all times • Murray Forestry Ltd will not keep data and records for longer than is necessary. • Murray Forestry Ltd will hold data and records in a secure environment with access restricted to those members of staff with a legitimate business requirement. No files containing personal data shall be left unattended and accessible on desks. • Murray Forestry Ltd will ensure that secure cabinets are available for active files and that secure storage is available for archive files. IT security is managed by reputable contracted IT provision. • When references are requested from Murray Forestry Ltd these will always be provided on a confidential basis to the person requesting the reference. • Murray Forestry Ltd will endeavour to maintain security of its electronic data by the installation of industry standard security procedures for external connections and the use of passwords and network access facilities to minimise the scope for inappropriate distribution of personal data within the organisation. • Murray Forestry Ltd may email contact periodically with news of relevant activities, opportunities and events. • Murray Forestry Ltd keeps all client contractual information in secure IT storage. • Murray Forestry Ltd disposes of data no longer required (ie. paper files) though a reputable contracted information disposal service. This ensures information is securely eradicated. • Murray Forestry Ltd does not share or sell personal information about contacts/customers with third parties for the purposes of marketing. • Murray Forestry Ltd maintains all financial records in line with strict internal financial controls that are

	subject to standard accounting procedures, not least the need to retain account records for seven years. **DATA PROTECTION POLICY** **POLICY STATEMENT** Murray Forestry Ltd will manage information in a way that: • Safeguards the confidentiality of commercially or personally sensitive information. • Shows respect and consideration to the subjects of the information or those who may be affected by its use. • Demonstrates professionalism and courtesy. • Does not breach equal opportunities legislation or related good practice guidance. • Complies with the Data Protection Act 1998, The Computer Misuse Act 1990, the General Data Protection Regulation 2018 (GDPR) and related good practice guidance. GDPR gives individuals more rights and requires organisations to be transparent about their activities with regards to personal data. Therefore, Murray Forestry Ltd will review and update all processes and procedures to reflect required compliance. • Does not expose Murray Forestry Ltd to prosecution, adverse publicity or damage to its reputation. Murray Forestry Ltd believes that its staff, clients, partners and stakeholders should have access to information on how it conducts itself. This means that unless information requested is considered commercially sensitive or personally confidential it will be made available on request. This will include information on: • Performance against operational targets • Quality Audit assessments • Policies and procedures • Non confidential reports The above is not exhaustive and Murray Forestry Ltd will action any request for information within the scope of this policy. **SCOPE AND AIM** The aim of this policy is both to ensure that all staff are aware of their particular responsibilities in relation to the

	Data Protection Act and GDPR and to inform stakeholders how Murray Forestry Ltd complies with the legislation. It is also to minimise the risk of the company breaching the legislation; thereby potentially damaging valued relationships and reputation. This policy covers all personal data and sensitive personal data held in electronic format or in relevant manual filing systems that is processed by Murray Forestry Ltd. It sets out how Murray Forestry Ltd will meet its obligation by: • Confirming the principles of data confidentiality • Confirming the standards Murray Forestry Ltd will observe in keeping data secure and relevant • Its detailed Privacy Notice (refer to Appendix 1) It applies to all staff and associates, volunteers and interns and relevant stakeholders. **STATEMENT OF PRINCIPLES** **Data Protection Principles** Murray Forestry Ltd will manage information in accordance with the Data Protection principles contained in the Data Protection Act 1998 and updated by the GDPR 2018. These represent the minimum standards of practice for any organisation with respect to personal data/sensitive personal data and state that it must be: • Processed fairly and lawfully and in a transparent manner in relation to the individual. • Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. • Processed for limited purposes and not in any manner incompatible with those purposes. • Adequate, relevant and not excessive, ie limited to what is necessary in relation to the purposes for which they are processed. • Accurate and kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate is erased/rectified without delay. • Not kept for longer than is necessary, ie with regards to personal data that permits the identification of the individual. The rights and freedoms of the individual must be safeguarded. • Processed in line with data subjects' rights.

	• Secure, ie processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised/unlawful processing and against accidental loss, destruction or damage using appropriate organisational measures. • Not transferred to countries that don't protect personal data adequately. Murray Forestry Ltd will comply with GDPR requirements by reviewing and creating (where necessary) additional internal processes for secure strong, processing and disposing of personal data and sensitive personal data and ensure this is integral to the company's quality management system. The Data Protection Act is concerned with two types of information: **PERSONAL DATA** (Definition: Information held on a relevant filing system which relates to a living individual who can be identified from the data). Processing of this data can only be carried out where one of the following conditions has been met: • The individual has given his/her consent. • It is necessary for the performance of a contract with the individual or for the taking of steps at the request of the individual with a view to entering into a contract. • It is a legal obligation. • It is necessary to protect the vital interests of the individual. • It is necessary in order to pursue the legitimate interests of Murray Forestry Ltd or third parties (unless it would prejudice the interests of the individual). In general the above conditions will be met where the processing is necessary for Murray Forestry Ltd's role and obligations as an employer. **Individual Rights** Any individual has the right to ask what information Murray Forestry Ltd holds about them and why it is being held. Murray Forestry Ltd will seek to respond to any inquiries about the new rights under the GDPR including:

	• Individual right of access to personal information records • Individual right to correct data • Individual right to be forgotten/for records to be deleted • Individual right to withdraw consent for processing at any time • Individual right to complain to the Information Commissioner's Office (ICO) **SENSITIVE PERSONAL DATA** (Definition: Data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activity). This data is not formally held by Murray Forestry Ltd and can only be processed under strict conditions which include: • Having the explicit consent of the individual • Being required by law to process the data for employment purposes • Needing to process the information in order to protect the vital interests of the individual or another • Dealing with the administration of justice or legal proceedings This type of information should only be held if one of the above conditions applies. The main data likely to be held under this category is regarding medical conditions relevant to role. Where this information is collected the specific consent to process the data will be sought from the individual. Ultimate responsibility for compliance with the Data Protection Act lies with Murray Forestry Ltd's Directors. **BREACH** Breach of data protection legislation is a criminal offence and potentially a civil offence and Murray Forestry Ltd will regard wilful or reckless breach of this policy as a disciplinary offence and such breaches will be subject to company disciplinary procedures. It is the duty of all staff to immediately inform a Director of any matter arising that involves, or is thought to involve, a breach of data protection legislation. Breach of data within the company

	will also be reported to those whose data may have been affected by the breach. **APPENDIX 1** **Privacy notice** • Murray Forestry Ltd requires its staff, directors and others who have access to Murray Forestry Ltd's information and communications facilities (eg temporary staff, consultants, etc) to comply with the principles of the Data Protection Act 1998 and the General Data Protection Regulation 2018 (GDPR) and maintain data confidentiality at all times • Murray Forestry Ltd will not keep data and records for longer than is necessary. • Murray Forestry Ltd will hold data and records in a secure environment with access restricted to those members of staff with a legitimate business requirement. No files containing personal data shall be left unattended and accessible on desks. • Murray Forestry Ltd will ensure that secure cabinets are available for active files and that secure storage is available for archive files. IT security is managed by reputable contracted IT provision. • When references are requested from Murray Forestry Ltd these will always be provided on a confidential basis to the person requesting the reference. • Murray Forestry Ltd will endeavour to maintain security of its electronic data by the installation of industry standard security procedures for external connections and the use of passwords and network access facilities to minimise the scope for inappropriate distribution of personal data within the organisation. • Murray Forestry Ltd may email contact periodically with news of relevant activities, opportunities and events. • Murray Forestry Ltd keeps all client contractual information in secure IT storage. • Murray Forestry Ltd disposes of data no longer required (ie. paper files) though a reputable contracted information disposal service. This ensures information is securely eradicated. • Murray Forestry Ltd does not share or sell personal information about contacts/customers with third parties for the purposes of marketing. • Murray Forestry Ltd maintains all financial records in line with strict internal financial controls that are

	subject to standard accounting procedures, not least the need to retain account records for seven years.
R Groom Tree Services	**Commitment** We are committed to the principles inherent in the GDPR and particularly to the concepts of privacy by design, the right to be forgotten, consent and a riskbased approach. In addition, we aim to ensure: •transparency with regard to the use of data •that any processing is lawful, fair, transparent and necessary for a specific purpose •that data is accurate, kept up to date and removed when no longer necessary •that data is kept safely and securely. **Staffing** Our Data Protection Officer (DPO), will maintain a commitment to best practice and inform and advise the company and monitor compliance. **Policy** Our privacy policy is available and a copy has been made available to all employees and to contractors and suppliers associated with this organisation. It forms part of the induction training of all new staff and follow-up sessions will be put in place if the legislation changes or further guidance is available. **Right to be forgotten** We recognise the right to erasure, also known as the right to be forgotten, laid down in the GDPR. **Subject access requests** We recognise that individuals have the right to access their personal data and supplementary information and will comply with the one month timeframe for responses set down in the GDPR. As a general rule, a copy of the requested information will be provided free of charge although we reserve the right to charge a “reasonable fee” when a request is manifestly unfounded or excessive, particularly if it is repetitive. If this proves necessary, the data subject will be informed of their right to contest our decision with the supervisory authority (the Information Commissioner’s Office (ICO)).

	As set out in the GDPR, any fee will be notified in advance and will be based on the administrative cost of providing the information. **Privacy** We will implement data protection "by design and by default", as required by the GDPR. Safeguards will be built into products and services from the earliest stage of development and privacy-friendly default settings will be the norm. explains our lawful basis for processing the data and gives the data retention periods. Individuals have a right to complain to the ICO. We have conducted a privacy impact assessment (PIA) to ensure that privacy risks have been properly considered and addressed. **Privacy Information Notices** We have put recognised procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of any personal data that is transferred to countries outside the EU. Diligence checks are carried out to ensure that such countries have the necessary safeguards in place, provide enforceable data subject rights and offer effective legal remedies for data subjects where applicable. **Children** The GDPR provides for special protection for children's personal data and we will comply with the requirement to obtain parental or guardian consent for any data processing activity involving anyone under the age of 16. Systems have been introduced to verify individuals' ages. **Data loss** If a data breach occurs that is likely to result in a risk to the rights and freedoms of individuals, the people affected will be informed as soon as possible and the ICO will be notified within 72 hours
TD Tree and Land Services Ltd	The ***EU General Data Protection Regulation ("GDPR")*** came into force across the European Union on 25th May 2018 and brought with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

	The 21st century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information. **Our Commitment** TD Tree & Land Services Ltd *('we' or 'us' or 'our')* are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection Bill. TD Tree & Land Services Ltd are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance. In order to ensure our full compliance with the new regulations TD Tree & Land Services Ltd performed the following tasks: • ***Information Audit*** - a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed. • ***Policies & Procedures -*** implementing new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: - ➢ ***Data Protection*** – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR. Accountability and governance measures are in place to ensure that we understand and adequately disseminate and

	evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals. ➢ ***Data Retention & Erasure*** – we have updated our retention policy and schedule to ensure that we meet the *'data minimisation'* and *'storage limitation'* principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new *'Right to Erasure'* obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities. ➢ ***Data Breaches*** – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow. ➢ ***Subject Access Request (SAR)*** – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate. • ***Privacy Notice/Policy*** – we have revised our Privacy Notice(s) to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information. • ***Obtaining Consent*** - we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and

	date records; and an easy to see and access way to withdraw consent at any time. • ***Data Protection Impact Assessments (DPIA)*** – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s). • ***Processor Agreements*** – where we use any third-party to process personal information on our behalf (*i.e. Payroll, Recruitment etc*), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (*as well as we*), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR. **Data Subject Rights** In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, we provide easy to access information via our Staff Handbook and in the office of an individual's right to access any personal information that TD Tree & Land Services Ltd processes about them and to request information about: - • What personal data we hold about them • The purposes of the processing • The categories of personal data concerned • The recipients to whom the personal data has/will be disclosed • How long we intend to store your personal data for • If we did not collect the data directly from them, information about the source • The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this • The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any

	direct marketing from us and to be informed about any automated decision-making that we use • The right to lodge a complaint or seek judicial remedy and who to contact in such instances **Information Security & Technical and Organisational Measures** TD Tree & Land Services Ltd takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction. **GDPR Roles and Employees** TD Tree & Land Services Ltd have designated Caroline Tempest as our Appointed Person for Data Protection. She is responsible for promoting awareness of the GDPR across the organization and ensuring the new policies, procedures and measures are implemented. TD Tree & Land Services Ltd understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our planning. We have implemented an employee training module provided to all employees and also forms part of our induction and annual training program.
Weir Forestry	We intend to work this contract on a paperless system with all data stored electronically. All devices used to store data are password and/or fingerprint protected to minimise the risk of access by third parties. Any personal data collected in the field is input directly to the relevant field form and not held in any other location until returned to contract manager and Scottish Forestry. Only those working on the survey have access to personal data, this is not shared with third parties and surveyors do not have access to data collected by each other unless this becomes relevant to field work where contact information may be shared between surveyors. All data is deleted from field devices at the end of the survey period and stored on computer thereafter to allow

	for any queries from the survey to be answered. This is held for approximately six months from completion of the final survey up to a maximum of one year from the initial Call-Off. A diary reminder is set at the time of the initial Call-Off to ensure that data is deleted no more than once year from this date. This is the General Data Protection Regulation (GDPR) Policy of Weir Forestry **CONTEXT AND OVERVIEW** **Key Details:** - Policy prepared by: **Redacted** - Approved by the partners on: 28 December 2015 - Policy became operational on: 28 December 2015 - Date of next review: 1 February 2020 **Introduction** Weir Forestry needs to gather and use certain information about individuals. These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law. **Key Details:** This data protection policy ensures Weir Forestry: - Complies with data protection law and follows good practice; - Protects the rights of staff, customers and partners; - Is open about how it stress and processes individuals' data; - Protects itself from the risks of a data breach. **Data Protection Law** GDPR 2018 describes how organizations including Weir Forestry must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.
To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

GDPR is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully;
2. Be obtained only for specific, lawful purposes;
3. Be adequate, relevant and not excessive;
4. Be accurate and kept up to date;
5. Not be held for any longer than necessary;
6. Processed in accordance with the rights of data subjects;
7. Be Protected in appropriate ways;
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection.

PEOPLE, RISKS AND RESPONSIBILITIES

Policy Scope

This policy applies to:

- The head office of Weir Forestry;
- All branches of Weir Forestry;
- All staff and volunteers of Weir Forestry;
- All contractors, suppliers and other people working on behalf of Weir Forestry.

It applies to all data that the business holds relating to identifiable individuals even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers;
- …plus any other information relating to individuals.

Data Protection Risks

This policy helps to protect Weir Forestry from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the business uses data relating to them.
- **Reputational damage.** For instance, the business could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with Weir Forestry has some responsibility for ensuring data is collected, stored and handled appropriately.

All those who handle personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The partners are ultimately responsible for ensuring that Weir Forestry meets its legal obligations.
- The data protection officer, **Redacted**, is responsible for:
    - Keeping the partners updated about data protection responsibilities, risks and issues.
    - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    - Arranging data protection training and advice for the people covered by this policy.
    - Handling data protection questions from staff and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data Weir Forestry holds about them (also called, “subject access requests”).
    - Checking and approving any contracts or agreements with third parties that may handle the business’ sensitive data.
- The IT manager, **Redacted**, is responsible for:
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
    - Performing regular checks and scans to

ensure security hardware and software is functioning properly.
    - Evaluating any third-party services the business is considering using to store or process data. For instance, cloud computing services.

- The marketing manager, **Redacted**, is responsible for:
    - Approving any data protection statements attached to communications such as emails and letters.
    - Addressing any data protection queries from journalists or media outlets like newspapers..
    - Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

GENERAL STAFF GUIDELINES

- The only people able to access data covered by this policy should be those who **need it for their work.**
- Data **should not be shared informally.** When access to confidential information is required it must be requested from one of the partners.
- **Weir Forestry will provide** training to help individuals understand their responsibilities when handling data.
- All data must be kept secure by taking sensible precautions and following the guidelines below.
- In particular, **Strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorized people, either within the business or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- If unsure about any aspect of data protection advice must be sought.

DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager.

When data is **stored on paper**, it should be kept in a

	secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason: - When not required, the paper or files should be kept **in a locked drawer or filing cabinet.** - Paper and printouts must **not be left where unauthorized people could see them,** like on a printer. - **Data printouts should be shredded** and disposed of securely when no longer required. When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts: - Data should be **protected by strong passwords** that are changed regularly and never shared between employees. - If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used. - Data should only be stored on **designated drives and servers**, and should only be uploaded to an approved cloud computing service. - Servers containing personal data should be **sited in a secure location**, away from general office space. - Data should be **backed up frequently**. Those backups should be tested regularly, in line with standard backup procedure. - Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones. - All servers and computers containing data should be protected by **approved security software and a firewall**. **DATA USE** Personal data is of no value to Weir Forestry unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft: - When working with personal data **the screens of computers should be locked** when unattended. - Personal data **should not be shared informally**. In particular it should never be sent by email, as this form of communication is not secure.

	- Data must be **encrypted before being transferred electronically**. The IT manager is responsible for sending data to authorized external contacts. - Personal data should **never be transferred outside of the European Economic Area**. **DATA ACCURACY** The law requires Weir Forestry to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Weir Forestry should put into ensuring its accuracy. It is the responsibility of all working those working with data to take reasonable steps to ensure it is kept as accurate and up to date as possible. - Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets. - Staff should **take every opportunity to ensure data is updated**. For instance, by confirming a customer's details when they call. - Weir Forestry will make it **easy for data subjects to update the information** Weir Forestry holds about them. For instance, via any business website. - Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database. - I is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months. **SUBJECT ACCESS REQUESTS** All individuals who are the subject of personal data held by Weir Forestry are entitled to: - Ask **what information** the business holds about them and why. - Ask **how to gain access** to it. - Be informed **how to keep it up to date**. - Be informed how the business is **meeting its data protection obligations**.

	If an individual contacts the business requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the data controller at weir.forestry@btinternet.com. The data controller can supply a standard request form, although individuals do not have to use this. Individuals will be charged £10.00 per subject access request. The data controller will aim to provide the relevant data within 14 days. The data controller will always verify the identity of anyone making a subject access request before handing over any information. **DISCLOSING DATA FOR OTHER REASONS** In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Weir Forestry will disclose requested data. However, the data controller will ensure the request is legitimate, seeking legal advice if necessary. **PROVIDING INFORMATION** Weir Forestry aims to ensure that individuals are aware that their data is being processed, and that they understand: - How the data is being used. - How to exercise their rights
2 Excel	The company (2Excel) Data Protection Policy has been added as a supporting document to the tender submission. All data acquired as part of fulfilment of the tender would adhere to the data protection policy. The policy has been put in place by 2Excel to set out its obligations regarding data protection and the rights of its data subjects in respect of their personal data under the General Data Protection Regulation. Data collected as part of any tender fulfilment (such as Tree Health Surveys) will be

	treated in the same manner as other data subjects such as employees, customers or contractors. The company also holds an ISO 9001:2015 Quality Management System Certificate. The Quality Management System includes the collection, processing, storage and dissemination of datasets. As a result, data collected as part of a fulfilment of tender would be managed under this approved system. **PURPOSE** The purpose of this Policy is to set out the obligations of 2Excel regarding data protection and the rights of its data subjects in respect of their personal data under the General Data Protection Regulation. **SCOPE** This policy will cover all data subjects which may include, but not limited to, employees, contractors, volunteers, customers and business contacts. **POLICY STATEMENT** The Regulation defines “personal data” as any information relating to an identified or identifiable natural person (a data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. This Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company. The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals. In drawing up this policy, due account has been taken of the following:

	General Data Protection Regulation (GDPR) which comes into force in the UK on 25th May 2018 and replaces the Data Protection Act 1998 **THE DATA PROTECTION PRINCIPLES** The Regulation sets out the following principles with which any party handling personal data must comply. All personal data must be: 1. processed lawfully, fairly, and in a transparent manner in relation to the data subject; 2. collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; 3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed; 4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay; 5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject; 6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. **LAWFUL, FAIR AND TRANSPARENT DATA PROCESSING** The Regulation seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

	1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes; 2. processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; 3. processing is necessary for compliance with a legal obligation to which the controller is subject; 4. processing is necessary to protect the vital interests of the data subject or of another natural person; 5. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; 6. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. **PROCESSED FOR SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES** The Company collects and processes the personal data set out in Part 14 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates with us). The Company only processes personal data either for the specific purposes set out in Part 14 of this Policy and for other purposes expressly permitted by the Regulation. The purposes for which we process personal data will be informed to data subjects at the time that their personal data is collected. **ADEQUATE, RELEVANT AND LIMITED DATA PROCESSING** The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 6, above. **ACCURACY OF DATA AND KEEPING DATA UP TO DATE** The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date

	when advised of changes by the data subjects. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate. **TIMELY PROCESSING** The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed. When the data is no longer required, all reasonable steps will be taken to erase it without delay. **SECURE PROCESSING** The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 15 and 16 of this Policy. **ACCOUNTABILITY** The Company's data protection officer is the HR Manager, contactable on **Redacted** All employees and contractors of 2Excel who may have access to or process personal data must abide by the principles of this policy. Every department Head of Department (HoD) is responsible for establishing and recording: a) The purposes for which the Company processes personal data; b) Details of the categories of personal data collected, held, and processed by the department; and the categories of data subject to which that personal data relates; c) Details (and categories) of any third parties that will receive personal data from the department and ensuring a relevant Data Protection Agreement is in place if required (speak to the Company's data protection officer for more information); d) Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards; e) Details of how long personal data will be retained by the department; and

	f) Detailed descriptions of all technical and organisational measures taken by the department to ensure the security of personal data. This information should be provided to the data protection officer and any changes should be advised as soon as practically possible. **PRIVACY IMPACT ASSESSMENTS** The Company shall carry out Privacy Impact Assessments when and as required under the Regulation. Privacy Impact Assessments shall be overseen by the Company's data protection officer and shall address the following areas of importance: 1. The purpose(s) for which personal data is being processed and the processing operations to be carried out on that data; 2. Details of the legitimate interests being pursued by the Company; 3. An assessment of the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed; 4. An assessment of the risks posed to individual data subjects; and 5. Details of the measures in place to minimise and handle risks including safeguards, data security, and other measures and mechanisms to ensure the protection of personal data, sufficient to demonstrate compliance with the Regulation. **THE RIGHTS OF DATA SUBJECTS** The Regulation sets out the following rights applicable to data subjects: • The right to be informed; • When collecting personal data, the data subject will be informed: • Details of the Company • The purpose(s) for which the personal data is being collected and will be processed, the legal basis justifying that collection and processing; • Where applicable, the legitimate interests upon which the Company is justifying its collection and processing of the personal data; • Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

	• Where the personal data is to be transferred to one or more third parties, details of those parties; • Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place; • Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined); • Details of the data subject's rights under the Regulation; • Details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time; • Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation); • Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; • Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences. The information set out above shall be provided to the data subject at the following applicable time: a. Where the personal data is obtained from the data subject directly, at the time of collection; b. Where the personal data is not obtained from the data subject directly (i.e. from another party): 1. If the personal data is used to communicate with the data subject, at the time of the first communication; or 2. If the personal data is to be disclosed to another party, before the personal data is disclosed; or 3. In any event, not more than one month after the time at which the Company obtains the personal data. **The right of access;** A data subject may make a subject access request ("SAR") in writing to the Company's data protection oficer at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within

	one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension). All subject access requests received must be forwarded to the Company's data protection officer. The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive. **The right to rectification;** If a data subject informs the Company that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension). In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification of that personal data. **The right to erasure (also known as the 'right to be forgotten');** Data subjects may request that the Company erases the personal data it holds about them in the following circumstances: • It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed; • The data subject wishes to withdraw their consent to the Company holding and processing their personal data; • The data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) • The personal data has been processed unlawfully;

	• The personal data needs to be erased in order for the Company to comply with a particular legal obligation Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request (this can be extended by up to two months in the case of complex requests, and in such cases the data subject shall be informed of the need for the extension). In the event that any personal data that is to be erased in response to a data subject request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so). **The right to restrict processing;** Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so). **The right to data portability;** The Company does not process personal data using automated means. **The right to object;** Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes. Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing

	override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims. Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith. Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest. **Rights with respect to automated decision-making and profiling;** In the event that the Company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the Company. The right described here does not apply in the following circumstances: g) The decision is necessary for the entry into, or performance of, a contract between the Company and the data subject; h) The decision is authorised by law; or i) The data subject has given their explicit consent. Where the Company uses personal data for profiling purposes, the following shall apply: j) Clear information explaining the profiling will be provided, including its significance and the likely consequences; k) Appropriate mathematical or statistical procedures will be used; l) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

m) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling

Personal Data

The following is a non exhaustive example list of how personal data may be collected, held, and processed by the Company:

1. Personal Data held about employees will be collected, held and processed for all elements of the employment relationship, including but not restricted to, payroll, communication, reference requests, health and safety and meeting the requirements of employment legislation.
2. Personal data about job applicants will be collected, held and processed for the purposes of processing applications, organising interviews, communicating outcomes with candidates and collecting statistical information about applicants.
3. Personal data about passengers will be collected, held and processed to meet all domestic and international travel, health and safety and communication requirements.
4. Personal data about clients/visitors/business contacts will be collected, held and processed for communication purposes and to meet health and safety requirements

Data Protection Measures

The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

1. Where personal data is sent via email, these should be encrypted or if encryption is unavailable, as a minimum password protected.
2. Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely. Please refer to our ICT provider for guidance.
3. Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

	4. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted; 5. Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data; 6. Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient **or sent using recorded delivery marked "Strictly Private and Confidential, Addressee Only"** 7. No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the appropriate HoD, copying in the Data Protection Officer. 8. All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar; 9. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Company or not, without the authorisation of the Data Protection Officer. 10. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time; 11. If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it; 12. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Company or otherwise. 13. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the Regulation (which may include demonstrating to the Company that all suitable

	technical and organisational measures have been taken); 14. All personal data stored electronically should be stored on the appropriate network drive as it will be backed up by our ICT providers. 15. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols; 16. Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords; 17. Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of the relevant department HoD to ensure that no data subjects have added their details to any marketing preference databases including, but not limited to, the Telephone Preference Service, the Mail Preference Service, the Email Preference Service, and the Fax Preference Service. Such details should be checked at least quarterly. **Organisational Measures** The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data: 1. All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy or enter into a Data Protection Agreement as required; 2. Only employees, agents, sub-contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company; 3. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

	4. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised; 5. Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed; 6. The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed; 7. All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of this policy (and/or Data Protection Agreement if applicable) and the Regulation; 8. All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of the Regulation. This will be contracted via a Data Protection Agreement; 9. All Data Protection Agreements will ensure that where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure. **Transferring Personal Data to a Country Outside the EEA** i. The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA. ii. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies: 1. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data; 2. The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection

	clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority; 3. The transfer is made with the informed consent of the relevant data subject(s); 4. The transfer is necessary for the performance of a contract between the data subject and the Company (or for pre-contractual steps taken at the request of the data subject); 5. The transfer is necessary for important public interest reasons; 6. The transfer is necessary for the conduct of legal claims; 7. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or 8. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register. **Data Breach Notification** i. All personal data breaches must be reported immediately to the Company's data protection officer. ii. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it. iii. In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the data protection officer must

	ensure that all affected data subjects are informed of the breach directly and without undue delay. iv. Data breach notifications shall include the following information: 1. The categories and approximate number of data subjects concerned; 2. The categories and approximate number of personal data records concerned; 3. The name and contact details of the Company's data protection officer (or other contact point where more information can be obtained); 4. The likely consequences of the breach; 5. Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.