

Table 1 – All incidents 2018/19
(All lines highlighted in yellow are included in Table 2)

Ref Number	Incident Type	Reported to ICO	Number Of People Affected
2018-5054	Minor: Data sent by email to incorrect recipient	No	1
2018-5068	Minor: Data sent by email to incorrect recipient	No	1
2018-5071	Minor: Data sent by email to incorrect recipient	No	500
2018-5074	Minor: Insecure webpage (including hacking)	No	1
2018-5075	Minor: Data sent by email to incorrect recipient	No	1
2018-5076	Minor: Data sent by email to incorrect recipient	No	126
2018-5089	Minor: Data sent by email to incorrect recipient	No	1
2018-6091	Minor: Insecure disposal of paperwork	No	40
2018-6113	Major: Insecure webpage (including hacking)	Yes	108
2018-6116	Minor: Data sent by email to incorrect recipient	No	400
2018-6125	Minor: Data sent by email to incorrect recipient	No	7
2018-6128	Minor: Data sent by email to incorrect recipient	No	15
2018-6143	Minor: Data sent by email to incorrect recipient	No	2
2018-6146	Minor: Data sent by email to incorrect recipient	No	1
2018-6153	Minor: Data sent by email to incorrect recipient	No	2
2018-6155	Minor: Data sent by email to incorrect recipient	No	1
2018-6156	Minor: Data sent by email to incorrect recipient	No	1
2018-6165	Minor: Data sent by email to incorrect recipient	No	4
2018-6173	Minor: Other technical or organisational failure	No	4
2018-6180	Minor: Data sent by email to incorrect recipient	No	1
2018-6192	Minor: Data sent by email to incorrect recipient	No	1
2018-6197	Minor: Data sent by email to incorrect recipient	No	2
2018-6202	Minor: Data sent by email to incorrect recipient	No	8
2018-6206	Minor: Other technical or organisational failure	No	93
2018-6208	Minor: Data sent by email to incorrect recipient	No	1
2018-6222	Minor: Other technical or organisational failure	Yes	200
2018-6227	Minor: Data sent by email to incorrect recipient	No	4
2018-6252	Minor: Failure to redact data	No	2
2018-6255	Minor: Data sent by email to incorrect recipient	No	2
2018-6268	Minor: Information uploaded to webpage	Yes	1
2018-6272	Minor: Other technical or organisational failure	No	11
2018-6279	Minor: Other technical or organisational failure	No	22

2018-6290	Minor: Other technical or organisational failure	No	1
2018-6312	Minor: Data sent by email to incorrect recipient	No	20
2018-6313	Minor: Other technical or organisational failure	No	1
2018-6316	Minor: Data sent by email to incorrect recipient	No	1
2018-7332	Minor: Data sent by email to incorrect recipient	No	1
2018-7336	Minor: Data sent by email to incorrect recipient	No	2
2018-7366	Minor: Other technical or organisational failure	No	1
2018-7372	Minor: Data sent by email to incorrect recipient	No	1
2018-7379	Minor: Data sent by email to incorrect recipient	No	1
2018-7387	Minor: Insecure webpage (including hacking)	No	1
2018-7424	Minor: Data sent by email to incorrect recipient	No	1
2019-8443	Minor: Failure to redact data	No	3
2019-8456	Minor: Data sent by email to incorrect recipient	No	1
2019-8496	Minor: Data sent by email to incorrect recipient	No	10
2019-8506	Minor: Data sent by email to incorrect recipient	No	2
2019-8509	Minor: Other technical or organisational failure	No	12
2019-8518	Minor: Other technical or organisational failure	No	1
2019-8531	Minor: Data sent by email to incorrect recipient	No	4
2019-9552	Minor: Insecure webpage (including hacking)	Yes	1
2019-9581	Minor: Data sent by email to incorrect recipient	No	1
2019-9582	Minor: Data sent by email to incorrect recipient	No	1
2019-9589	Minor: Data sent by email to incorrect recipient	No	1
2019-9590	Minor: Data posted or faxed to incorrect recipient	No	14
2019-9592	Minor: Data posted or faxed to incorrect recipient	No	2
2019-9597	Minor: Failure to redact data	No	10

Appendix ii

Table 2 - Incidents reported to ICO / over 100 people affected/ more than a minor incident

Report no.	Summary	Business area	Incident Type	Number Of People Affected	Reported to ICO	Containment and Mitigation
2018-5071	An email issued manually to some users of the eDevelopment.scot service to advise of portal changes was sent in error from the 'carbon copy' field instead of the 'blind carbon copy' field. This error was discovered when a recipient contacted the SG.	Planning and Architecture Division	Minor: Data sent by email to incorrect recipient	500	No	An apology was issued and recipients asked to delete the email. After review, short-term changes to the processes have been put in place and a longer-term solution is being sought.
2018-5076	The business area sent an email to 276 students interested in applying to the Government Operational Research Service, but sent it from the 'carbon-copy' field rather than the 'blind-copy' field. 126 of these email addresses contained personal names.	Communities Analysis Division	Minor: Data sent by email to incorrect recipient	126	No	The business area tried to recall the email but it was unsuccessful. They decided not to inform all of the data subjects, but did reply to one student who had replied to the email mentioning that names were visible.
2018-6113	The Resourcing Team received an email from a member of the public, informing us that a link on the Work for Scotland website was a live link to the Vacancies Online login page	People Development Division	Major: Insecure webpage (including hacking)	108	Yes	Business area advised to review website security and will be part of wider SG review. The link was removed and Vacancies Online access was withdrawn from everyone except for SG's Resourcing team. A 100% check has been put in place to ensure that no incorrect links are included in job adverts.
2018-6116	Planning & Architecture carried out testing of an upcoming change in the 'pre-production' eDevelopment portal. In notifying users of this test an email was issued that did not 'blind copy' the recipients. [This error occurred because the checking procedure was not followed.]	Planning and Architecture Division	Minor: Data sent by email to incorrect recipient	400	No	An apology email was issued to each user and the business area reviewed their procedures again. We have subsequently subscribed to https://www.notifications.service.gov.uk/ to avoid repeating the error.

2018-6222	A procured service contractor for Scotland House in London, uses a cloud-based programme to process financial transactions. This system was hacked. The system contains details of Scottish companies who use spaces in Scotland House for business reasons. Information the hackers would have been able to access are available publicly. Business emails were part of that information. No sole traders were included in that list of businesses.	Scottish Government Office London	Minor: Other technical or organisational failure	0	Yes	Conversations regarding contract management were being taken forward by the Scotland House team. Input provided by the data protection team. The data processor notified the ICO before notifying us. The contract management issues arising from this and the data controller-data processor arrangements and associated reporting are being taken forward by Scotland House team and processes for reporting have been improved.
2018-6268	Mr P asked for information relating to a complaint he made about a public sector body in Scotland. He is mentioned in the papers released to him. Reference to him was not redacted as he is also the requestor of the information. His name therefore was shown when the FOI was published on the SG website.	Workforce, Infrastructure and Reform	Minor: Information uploaded to webpage	1	Yes	Breach has been contained and subject has accepted complaint process. SG processing improvements have been implemented.
2019-9552	Information held by the Energy Saving Trust on behalf of SG (1.2 million energy performance certificates) were accessed by circumventing the 'captcha' process. The information was in pdf format, and relates to building construction information, it is not personal data.	Building Standards	Minor: Insecure webpage (including hacking)	0	Yes	The business area are reviewing position of classing buildings as non-personal data post GDPR. The ICO took no action in this incident.