FREEDOM OF INFORMATION, DATA PROTECTION AND TRANSPARENCY: ANNUAL REPORT 2019/2020

To: Civic Affairs Committee	**14th October 2020**
Report by:	**Madelaine Govier** **Data Protection Officer & Information Governance Manager** **(3C Shared Services - Information Governance)** **Email: Madelaine.govier@3csharedservices.org**
Wards affected	**All**

1. INTRODUCTION

1.1 The purpose of this report is to provide an update on Information Governance activity and performance during 2019/20 (April 2019 - March 2020).

1.2 It provides:

- An overview of the current arrangements in place to monitor the Information Governance arrangements at the Council including Data Protection Compliance and Information Security / Cyber Security Compliance.

- An update on performance relating to:
  - Freedom of Information (FOI) Act / Environmental Information Regulations (EIR) Requests
  - Data Subject Access Requests
  - Personal Data Breaches
  - Uptake of Information Governance Training

2. RECOMMENDATIONS

2.1 The Committee is asked to note the report.

3. BACKGROUND

3.1 Information is a vital asset and needs to be managed securely by the council. Appropriate policies, guidance, accountability and structures must be in place to manage the council's information legally, securely and effectively in order to minimise risk to the public and staff and to protect its finances and assets.

3.2 Information Governance describes the holistic approach to managing information by implementing processes, roles and metrics to transform information into business assets. This includes coverage around access to information, data quality, information management, information security and information sharing, data privacy and Data Protection compliance.

4. ORGANISATIONAL ARRNAGEMENTS

4.1 The Information Governance Service for the City Council, South Cambs District Council and Huntingdonshire District Council is currently provided by 3C ICT Shared service hosted by Huntingdonshire District Council. The Information Governance (IG) Team lead on Information Requests, Data Protection Compliance, Data Privacy and provide additional advice around Information Management; whilst the 3C ICT Network team provide support on Information Security.

4.2 The IG Team consists of six members, four of whom, including the current Data Protection Officer (DPO), joined this year. The DPO is a statutory role required by Local Authorities, and is responsible for leading the IG team. As a shared service, the team leader is also the DPO for all three Authorities.

4.3 Updates on IG arrangements across Cambridge City Council are provided to the Information Security Group (ISG). This Group is designed to facilitate the necessary engagement and to ensure the relevant accountability of staff across the various Services and assist in driving any improvements required. It is chaired by the Senior Information Risk Owner (Fiona Bryant) and comprises of number of managers / heads of services across most service areas within the Council.

4.4 The Information Security Group meets quarterly and last met in early November 2020

5. DATA PROTECTION COMPLIANCE

5.1 The team have carried out a review of the Data Protection arrangements this year to determine the areas for priority action.

5.2 The main areas covered included: Lawfulness, Fairness and Transparency, Individual Rights, Accountability and Governance, Data Security, International Transfer and Breaches. Each area consisted of a number of sub-categories. See **Appendix A** for details.

5.3 In summary, a key finding from the review was that, whilst appropriate procedures were generally in place, there are some gaps and improvements to be delivered in document management and access. Improvements are required in the following areas for example:

Area	High Level Finding	Risk	Actions needed
Information Asset Registers / Flows	Although Information Asset records are held by Service areas, Information Governance do not currently hold a central repository Information Asset records also should be reviewed regularly to ensure information is accurate.	The risk is delays to responses to information requests, and inaccurate responses if central repository does not contain up to date information.	Update review of existing information to ensure this is up to date; and collate this centrally
Records of Processing (Article 30)	Although the Information Asset Register does collect most of the information required for Article 30; this is not held centrally; in addition to this more information would be required on disclosures and transfers.	Risk of inappropriate transfer of data	Review existing information to ensure transfers and method of these are documented.
Policies	Ensuring clear accessibility for **all** staff to up to date policies, including, for example IT Policies located within a	The risk is staff may not be aware of updates	Review of policies and publication ensuring clear access to all.

	repository (Protocol Policy)		
Training Arrangements	Compulsory e-learning was undertaken for all City staff - pre GDPR. There is currently a requirement to undertake this every 2 years. All new starters have also have e learning as part of their induction process.	Although compliant with legislation, timing for refresher training is not currently in line with other partners in the public sector. This can present issues when signing up to Information Sharing Agreements.	Review IG training provision & reporting for induction, refresher, specific roles.
Information Sharing Arrangements	No central register for the data sharing agreements signed by Council	Lack of clear central visibility on appropriateness of contracts / sharing agreements already in place. May lead to compliance risk	Central information Sharing Log is to be created. The Information Asset Register work, is also likely to identify where additional agreements/contracts may be needed.
Incorporation of Privacy by Design in Projects	The Data Privacy Impact Assessment (DPIAs) are being completed but Information Governance require further assurance that all those required are in place. DPIAs are currently treated as a standalone document to be completed at project initiation.	Possible risk that privacy risks may either not identified / identified in a timely manner.	The DPIA process needs to be better documented and integrated with Project management / Change Processes.

5.4 The actions required to address these issues have been factored into the ongoing IG forward plan 2020/21.

5.5 Updates to monitor the status and progress on this will be provided to the City's Information Security Group (ISG).

6. INFORMATION SECURITY COMPLIANCE / CYBER ESSENTIALS

6.1 In an increasingly connected world, cyber security plays a critical role in not only securing systems and data, but also gives the assurance in sharing data.

6.2 The council has continued to invest, develop and improve its cyber security position covering systems, processes and procedures. Over the past 12 months, 3C ICT have been monitoring and managing cyber security risks across a number of different areas. (See **Appendix B**)

6.3 Last year's report to Committee referenced a proposal to adopt Cyber Essentials Plus as a framework for security assurance. Whilst Cyber Essentials is a simple but effective scheme to provide cyber security assurance, however, it only covers 5 basic controls.

6.4 Threats and risks to our organisation come in many shapes and sizes. In order to cover the areas of risks that an organisation of our size and type should be routinely managing, 3C ICT have instead adopted the 10 steps to Cyber Security (NCSC10) which goes further than Cyber Essentials.

The approach is supported and backed by the NCSC (National Cyber Security Centre) who are the national information governance authority. The Cyber Essential controls are still covered, but in addition, more enterprise level risks are catered for within the NCSC10 steps approach. Using this approach, we are now able to measure the rate and level of improvement in cyber security risk.

6.5 Throughout FY 2019 to 2020 we have documented improvements in a number of key cyber risk areas including Risk management methodology, Incident Management, Systems Monitoring, user education and awareness and Remote Working. Across all the 10 themes the RAG statuses are green and amber, with four being Amber and six being Green. See **Appendix B** for summary of themes and RAG status.

6.6. The four residual amber areas include risk management, incident management and user education and awareness. The rationale behind the amber status for these four areas is the following:

- Risk management – We're only a little over 6 months into this method of monitoring and scoring the Cyber Security risks. This will be considered green when we have a consistent and repeatable process for 12 months
- Incident Management – requires further testing to be considered mature
- User education and awareness – Training plan and reporting and monitoring to be agreed by Information Security Groups to achieve green. In the meantime,

regular comms about current trends and threats mitigates this. IT technical training is underway for specific posts.

- Monitoring – consolidation of tools and completion of project to improve management and monitoring with specific part of the infrastructure

We have an action plan in place which is designed to achieve green status on all 10 steps by end March 2021.

6.7 The intention is to use the detailed information and evidence gathered as part of this approach to complete the cyber essentials assessment in any case , however, because this approach is also endorsed by the Cabinet Office / PSN accreditation authority, we believe that following the 10 steps to cyber security is a more suitable approach to measuring and assessing information assurance.

6.8 We are planning an independent review of this assurance assessment which will be completed by end March 2021 to ensure that we have external verification on the assessment

7. PERFORMANCE UPDATE

7.1 FREEDOM OF INFORMATION / ENVIRONMENTAL REQUESTS

The public has the right of access to information held by the Council under the Freedom of Information Act. The Freedom of Information Act (FOI) works alongside the Environmental Information Regulations (EIR).

7.2 Freedom of Information requests relate to requests for information that are not dealt with as part of the day-to-day business processes. Service areas are responsible for responding to requests and 3C ICT Information Governance Team manages the process, provide support and ensure compliance. The Council works to a target of 90% response compliance within 20 days (statutory requirement) as advised by the Information Commissioner. We achieved 88%. Reasons for this included: -

Service Areas not responding to requests for data on time and in some cases, FOI requests were not recognised as FOIs. The importance of responding to these on time and correctly as well as the importance of undertaking training this is being reinforced through the Information Security Group Meetings. In addition, the escalation process is being reviewed to see if any improvements can be made.

This report relates to those formally processed requests.

7.3 For the year 2019/20 (April – March) the council received a total of 716 requests under FOI and EIR, representing a 21.5% decrease in the number of requests received in 2018/19.

7.4 **Appendix B** demonstrates the year on year trend in the number of FOI requests since 2013/2014.

7.5 There are services which receive a high percentage of FOIs.
Appendix C shows the numbers and the percentages per service.

There are six departments (Environmental, planning, IT, Housing, Commercial and Revenues & benefits) with significant numbers of requests.

7.6 The IG team have recently developed reports, which will be shared with the Information Security Group on a quarterly basis, to understand trends, and to help departments focus on what should be uploaded onto their publication scheme

8.1 INDIVIDUAL DATA REQUESTS

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (GDPR). Data protection is primarily concerned with personal data about individuals rather than general information.

8.2 The Information Governance Team coordinate requests relating to individuals rights such as right to request access to the personal data the Council holds, right to erasure, right to rectification as well as third party requests for personal data such as from the Police or to prevent or detect fraud .

Appendix D includes the performance data related to this area.

There were 27 requests made during the year, of which 23 were responded to within target date. Reasons for delays included lack of awareness in recognising what constituted a Data Subject Access Request; establishing whether a request was valid and delays information being supplied by the service areas. The need for training of all staff is being reiterated through ISG, as well as additional training for Information Champions being given as appropriate.

9. PERSONAL DATA BREACHES

9.1 The guidance on notification of data breaches under the Data Protection Act / GDPR is that where a breach incident is likely to result in risk to the rights and freedoms of individuals, the Council must inform the ICO within 72 hrs and if it's likely to result in high risk to rights and freedoms of individuals, the Council has a lawful duty to inform the individuals without undue delay.

9.2 As a result the IG team have established a framework to ensure that each reported incident is assessed for:

- The potential detriment and adverse effect to the data subject. This includes emotional distress and information about the private aspects of a person's life becoming known to others.

- The extent of detriment. Which could depend on the volume of the data and its sensitivity.

This is performed by the IG team when an incident is logged by a Service Area.

9.3 The IG Team have also developed a register to log incidents / near misses relating to personal data. This allows trends to be identified, with the view to establish if any specific training needs are required or if any actions are needed to enhance the current measures to prevent the likely reoccurrence.

9.4 **Performance Data – Data Breaches**
Although 10 incidents were reported in 2019/20 (April 2019 – Mar 2020), None of these met the threshold for reporting to the ICO. A breakdown of these is provided in **Appendix E**.

9.5 In all instances, immediate steps were taken by officers to mitigate the incident, once known. Examples included contacting incorrect receiver of emails from the recipients of the email and those affected and removing documents from the Council's website.

9.6 A quarterly update on incidents is now provided to the ISG to ensure visibility and ensure any improvements needed are discussed and followed through as appropriate.

10 TRAINING

10.1 To ensure organisational compliance with the law and relevant guidance relating to Information Governance (IG), staff must receive appropriate training.

10.2 In 2018, when the GDPR legislation was implemented, staff underwent compulsory training via the e-learning module, or for operational staff, via videos shown during team meetings. At the City Council, it was proposed that staff completed training every two years. As a result, a vast majority of staff would be expected to retake the module this year; monthly reminders are currently being sent out via the HR team as appropriate.

10.3 In addition to this bi-annual refresher, all new starters who manage confidential information are expected to undertake training on handling confidential information.

10.4 The new IG Team intend to provide quarterly updates on training uptake to the ISG.

11. CONSULTATIONS

Senior managers have been consulted in the production of this report.

12. CONCLUSIONS

The Council takes transparency issues seriously and is broadly compliant with the legislation. A number of measures have been put in place to increase the Council's performance in these areas, and to reduce the risk of breaches in compliance with the legislation.

Officers will continue to review practice, learning from 3C ICT partners and others to strive to continually improve performance, serve residents better and reduce the council's exposure to risk.

13. IMPLICATIONS

(a) **Financial Implications**
No decisions with financial implications are proposed in this report.

(b) **Staffing Implications**
Staff will continue to be supported to understand and meet their obligations regarding transparency issues, including through the roll-out of the new FoI tracking software.

(c) **Equality and Poverty Implications**
This report does not propose decisions with equalities impacts, so and EqIA has not been produced.

(d) **Environmental Implications**
No decisions with environmental implications are proposed in this report.

(e) **Procurement**
N/a

(f) **Consultation and communication**
As set in the body of the report, the need for vigilance and training on data protection and related matters has been communicated to managers and staff regularly.

(g) **Community Safety**
N/a

14. BACKGROUND PAPERS

None

15. APPENDICES

Appendix A	Scope and Categories for Data Protection Gap Analysis
Appendix B	Areas for monitoring and managing cyber security risks
Appendix C	Yearly trends of FOI Requests received by Cambridge City Council (Numbers and Percentage of FOI responses responded to within 20 working days, and Complaints)
Appendix D	Breakdown of FOI Requests by Service Area (Percentage, Number of Requests, Compliance Levels)
Appendix E	Individual Rights Requests (Subject Access Requests)
Appendix F	Personal data breaches

16. BACKGROUND PAPERS

None

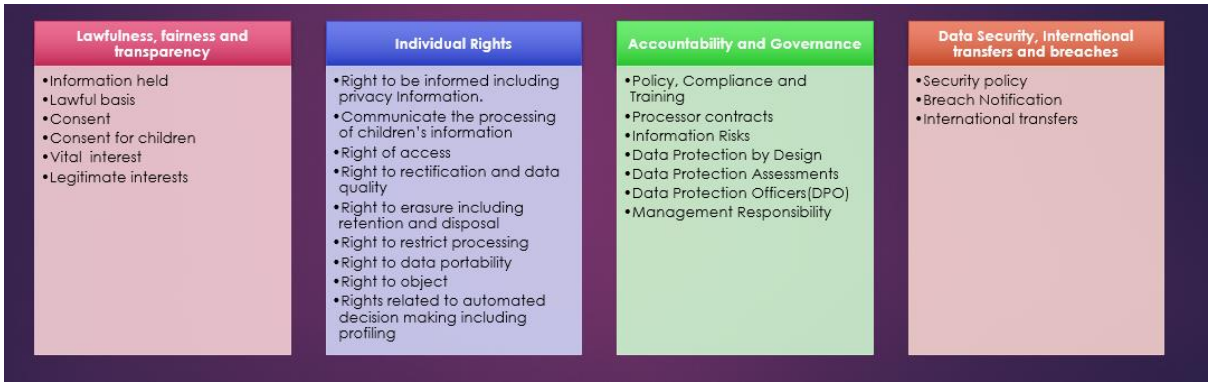
17. REPORT DETAILS AND CONTACT

Report: **Freedom of Information, Data Protection and Transparency: Annual Report 2019/2020**	Drafted: 1st September 2020 Last Revision: 1st September 2020
The author and contact officer for queries on the report	Information Governance Manager / Data Protection Officer **infogov@3csharedservices.org**

APPENDICES

APPENDIX A:

SCOPE AND CATEGORIES FOR DATA PROTECTION GAP ANALYSIS



APPENDIX B:

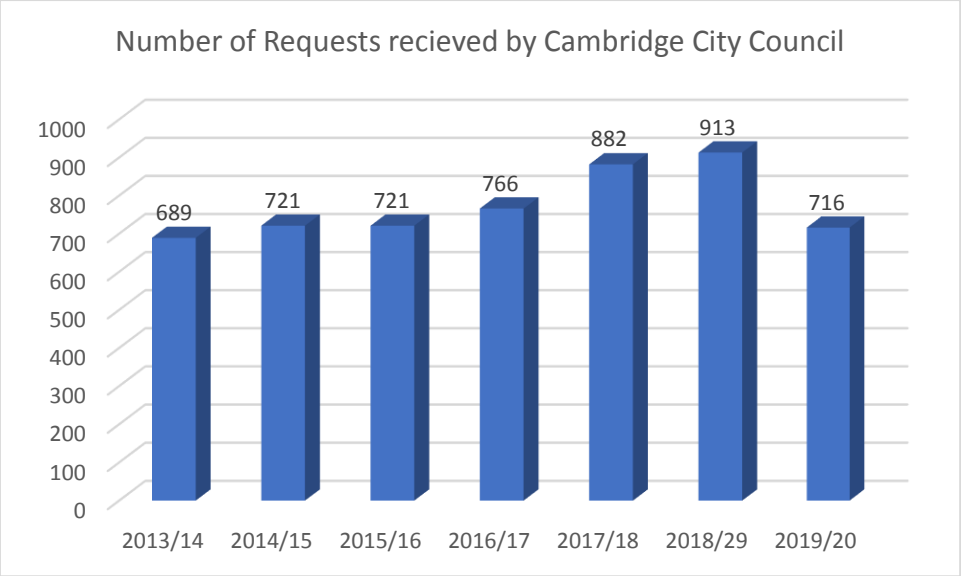
AREAS FOR MONITORING AND MANAGING CYBER SECURITY RISKS.

10 Steps Theme	Rating	RAG	Direction of travel
Risk Management	5	AMBER	↑
Secure Configuration	7	GREEN	↔
Network Security	7	GREEN	↑
Managing user privileges	7	GREEN	↔
Incident management	5	AMBER	↑
User education and awareness	5	AMBER	↑
Malware prevention	8	GREEN	↔
Monitoring	6	AMBER	↔
Removable media controls	8	GREEN	↔
Remote and mobile working	7	GREEN	↑

APPENDIX C:

YEARLY TREND OF FOI REQUESTS RECEIVED BY COUNCIL

a) NUMBER OF FOI REQUESTS RECEIVED (YEARLY)



b) COMPLIANCE LEVEL

Year	Number of Requests	% of requests responded to in 20 working days	% of requests responded to outside of 20 days target	ICO Target (%)
2013/14	689	92	8	85
2014/15	721	84	16	85
2015/16	721	91	9	85
2016/17	766	87	13	90
2017/18	882	90	10	90
2018/29	913	91	9	90
2019/20	716	88	12	90

c) FOI/EIR Complaints / Internal Reviews

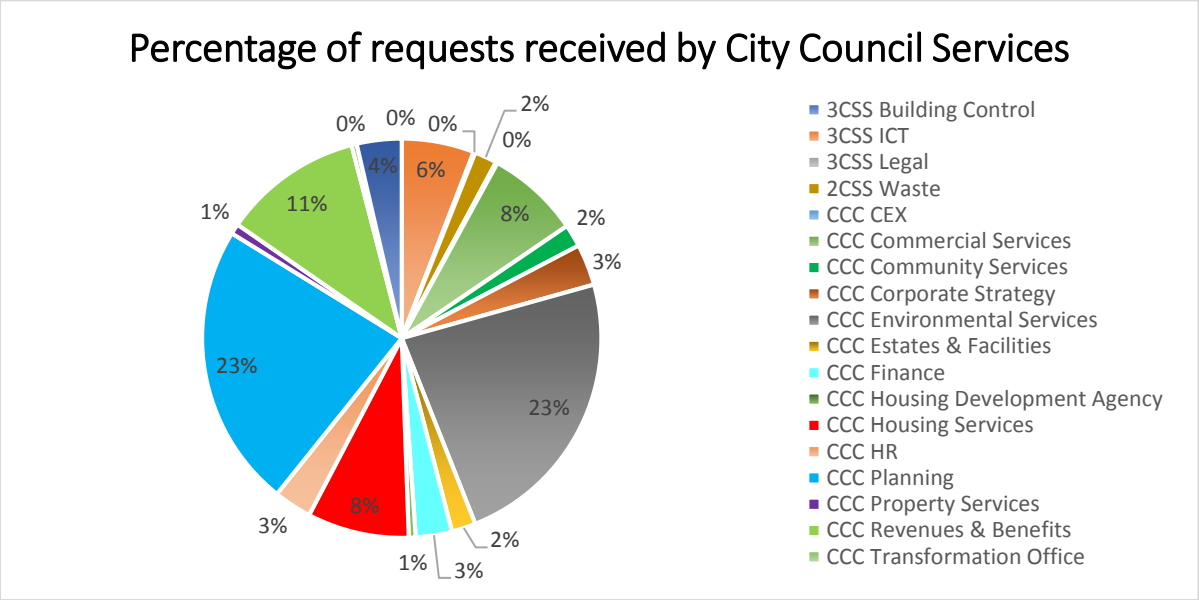
	Received	Compliance with time frame
Internal Reviews / Complaints	4	4
ICO Investigations	1	1

Whilst these have been investigated by the regulator (ICO) these have resulted in no action or they have found in the Councils favour.

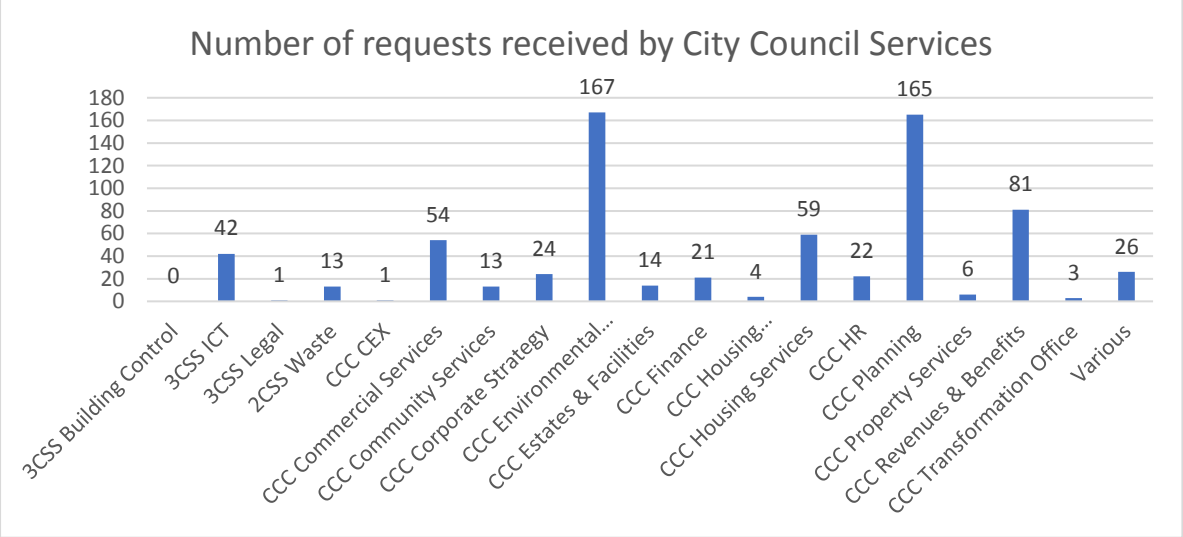
APPENDIX D:

BREAKDOWN OF FOI REQUESTS BY SERVICE AREAS

a) Percentage of Requests received by each Service Area



b) Numbers of Requests responded to by each area



c) Compliance level by each area

Service	Received	Response in 20 working days	% responded to in 20 working days	Average response time (working days)
3CSS Building Control	0	0	0	0
3CSS ICT	42	29	69%	23.5
3CSS Legal	1	0	0%	23.0
2CSS Waste	13	9	69%	21.2
CCC CEX	1	1	100%	20.0
CCC Commercial Services	54	53	98%	8.7
CCC Community Services	13	13	100%	8.8
CCC Corporate Strategy	24	23	96%	14.3
CCC Environmental Services	167	158	95%	13.1
CCC Estates & Facilities	14	9	64%	19.2
CCC Finance	21	18	86%	14.0
CCC Housing Development Agency	4	3	75%	24.8
CCC Housing Services	59	56	95%	13.6
CCC HR	22	22	100%	18.3
CCC Planning	165	131	79%	17.2
CCC Property Services	6	5	83%	17.7
CCC Revenues & Benefits	81	79	98%	9.9
CCC Transformation Office	3	2	67%	34.3
Various	26	21	81%	18.3
	716	**632**	**88%**	

APPENDIX E:

Individual Rights Requests

This includes other requests other formal requests for information (other than FOI/EIR)

E.g. Subject Access Requests, Erasure Requests

Other Requests	Received	Compliance with time frame
Subject Access Requests (SAR) (including Erasure Requests, etc.)	27	23
SAR Complaints	0	-

APPENDIX F:

PERSONAL DATA BREACHES

Personal data breaches recorded in 2019/20 (April 2019 – Mar 2020) by Category.

Type of Incident (Category)	Number	Reported to ICO
Documents sent in error to wrong recipient in post	5	Not reportable to ICO
Personal details inappropriately disclosed (e.g. via email/ shared)	3	Not reportable to ICO
Documents lost in transit	1	Not reportable to ICO
Total	10	