FREEDOM OF INFORMATION, DATA PROTECTION AND TRANSPARENCY: ANNUAL REPORT 2020/2021

To: Civic Affairs Committee	**22 September 2021**
Report by:	**Eleanor Dent** **Acting Deputy Data Protection Officer/ Senior Information Governance Specialist** **(3C Shared Services - Information Governance)** **Email: Eleanor.Dent@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 2020/21 (April 2020 - March 2021).

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 Incidents
  - 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 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 seven members, including the current Data Protection Officer (DPO). 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 information governance 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 Director and Senior Information Risk Owner (SIRO), Fiona Bryant and comprises of number of managers / heads of services across most service areas within the Council.

4.4 The Information Security Group agreed its Terms of Reference in February 2021. The purpose of the group is to provide SLT with assurance on information governance arrangements, ensure compliance with relevant legislation and council policies, and ensure that council services implement any actions necessary to ensure compliance.

4.5 The Information Security Group meets quarterly and last met in May 2021.

5. DATA PROTECTION COMPLIANCE

5.1 The team have built on last year's review of the Data Protection arrangements this year.

5.2 The Information Governance team have continued to focus on the key areas identified in 2019/20, including Lawfulness, Fairness and Transparency, Individual Rights, Accountability and Governance, Data Security, International Transfer and Breaches. Each area consists of a number of sub-categories. See **Appendix A** for details.

5.3 Following on from the priority areas identified in 2019/20 the Information Governance team have carried out improvements in the following areas.

Area	2019/20 Actions	Risk	Update on actions for 2020/21
Information Asset Registers (IAR) / Flows	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.	Information Asset Registers have been reviewed by all services.
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	Data flows identified under IAR review form baseline of records of processing.
Policies	Ensuring clear accessibility for **all** staff to up to date policies, including, for example IT Policies.	The risk is staff may not be aware of updates	Acceptable Use policy updated and signed off by ISG. New policy will be circulated by HR with

			compliance to monitor compliance.
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.	If timing for refresher training is not in line with other public sector partners this can present issues for public sector information sharing agreements.	Requirement to undertake refresher training every 12 months, bringing Council in line with other public sector partners. GDPR training must be undertaken within the first 10 days as part of new starter induction process. Compliance with training reported to all services quarterly via ISG.
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 has been created. Multi-agency Covid response working governed by information sharing agreements. Information Asset Register review identifying where additional agreements/contracts are needed.
Incorporation of Privacy by Design in Projects	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.	Information governance is integrated into the Council's Project development process as part of the Quality Assurance Group. This enables the IG team to give and early warning of DPIAs in projects. es.

5.4 Updates to monitor the status and progress of these actions are provided to the City's Information Security Group (ISG).

6. INFORMATION SECURITY COMPLIANCE / CYBER ESSENTIALS

6.1 Cyber Security continues to play an important role every day and routine business processes. Integration of systems and sharing of information and data across multiple platforms requires the council to maintain safe and secure systems providing assurance to residents, members of public and partner agencies.

6.2 The council has continued to invest, time effort and resource into managing and mitigating cyber security risks and threats. 3C ICT have carried on developing and improving cyber security against the backdrop of continually evolving threats. Particularly over the last 12 months where global incidents have become more frequent.

6.3 Even though Cyber Essentials is not as comprehensive as 10 steps (only covers 5 basic controls) The assessment process is under way and we are awaiting feedback from the submission. The NCSC 10 Steps will remain as the principal method of assessing our cyber security position, however, Cyber Essentials will benefit from this.

6.4 Over the last year there has been a significant growth in cyber criminality in the form of high profile campaigns including the one against Solarwinds. Each threat creates additional crucial but time consuming checks to ensure that the councils environment remains protected and secure.

The COVID-19 pandemic has had an unprecedented impact with the council staff having to adapt to new ways of working, including the change to standard working practices and the shift to working remotely. With Virtual Private Network (VPN) software always being a target, newly uncovered vulnerabilities in the software are having to be patched and updated frequently whilst staff continue to work remotely and 3C ICT minimising disruption to the service.

6.5 Throughout the last FY 3C ICT have continued to improve the statuses of the themes identified in the National Cyber Security Centre (NCSC) 10 Steps to Cyber Security. The high profile global incidents relating to ransomware impacting networks due to vulnerabilities of email systems, the policies and processes in place for patching has meant that 3C ICT have been able to patch the councils environment or mitigate the risks as soon as the vulnerabilities are released. See **Appendix B** for summary of themes and RAG status.

6.6 Last year it was reported that four areas were in amber. Of this four, two have now moved to green and although two are still amber improvements have been made in each area. The themes that have remained green still required significant time, effort and resource to maintain the position through the year due to the

rapidly changing threat and risk environment nationally and globally. The rationale behind the status for these four areas is the following:

- Risk management – This area has now matured and moved to green this is supported by the independent assessment of the risk management approach. Cyber security updates are provided to the Shared Services Board as well as the Information Governance Committee. 3C ICT have submitted the necessary forms for Cyber Essentials and although Cambridge City have PSN compliance, 3C ICT are working with the Cabinet Office for a single submission for all 3 partners.
- Incident Management – Although still regarded as amber. This area has improved with specialist cyber security training being completed and improved reporting and response to incidents. Process and procedures are in place and being used for dealing with cyber security incidents with the relevant bodies (National Cyber Security Centre, Information Commission Office, Action Fraud) all being notified when required. 3C ICT are continuing to promote user awareness and the importance of reporting any incidents.
- User education and awareness – This area has now moved to green. All staff are required to complete cyber security training when employment starts. Over the next year 3C ICT will testing the effectiveness of the training to ensure that it is relevant and to identify areas that still need improving. This is subject to a bid approval for the next FY.
- Monitoring – Although the work to complete the consolidation of tools is still ongoing (Due to other priorities COVID-19 response related) additional processes and procedures have been successfully developed and implemented in order to continue improvements in this area.

6.7 3C ICT have been working with the Cabinet Office and have agreed a more favourable approach to the annual PSN accreditation with the move to a single submittance for all 3 partners rather than a single submission for each. This will see 3C ICT as one of the early adopters and is the preferred way of working for the Cabinet Office.

6.8 Late 2020 3C ICT undertook an independent cyber security review. Among the good practices identified were that NCSC 10 Steps to Cyber Security had been identified, were being followed and reported on.

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, provides support, and ensures compliance.

The Council works to a target of 90% response compliance within 20 days (statutory requirement) as advised by the Information Commissioner. **We achieved 95% in 2020/21.**

This report relates to those formally processed requests.

7.3 For the year 2020/21 (April – March) the council received a total of 525 requests under FOI and EIR, representing a 27% decrease in the number of requests received in 2019/20.

7.4 **Appendix C** demonstrates the year on year trend in the number of FOI requests since 2014/2015.

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

There are three departments with significant numbers of requests. These are Environmental Services, Greater Cambridge Shared Planning and Revenues and Benefits Service.

7.6 Freedom of Information request volumes and performance are reported quarterly as part of the Corporate Performance reporting. Compliance reports are also reported to the Information Security Group to understand trends, and to help departments focus on their compliance.

8.1 PERSONAL DATA RIGHTS REQUESTS

The UK left the EU on 31 January 2020, and the General Data Protection Regulation (GDPR) was replaced by the UK GDPR. The UK GDPR retains the key principles, rights and obligations of the EU GDPR, and alongside the Data Protection Act 2018 forms the basis of Data Protection regulations in the UK. Data protection applies to information relating to living individuals and the regulations govern how the Council uses this information.

8.2 As a data controller the Council is responsible for ensuring that it meets the obligations of the Data Protection Regulations. The regulations give individuals specific rights over their information.

8.3 The Information Governance Team coordinate requests relating to individuals rights such as right to request access to the personal data the Council holds

(subject access), 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 E 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. Many of the delays to requests have been due to the limitations that have come from working from home, including accessing paper files, and providing responses in hard copies for those subjects who could not receive electronic files.

8.4 One rights request was escalated to the Information Commissioner's Office. This was resolved without further investigation from the ICO.

9. PERSONAL DATA INCIDENTS

9.1 The guidance on notification of data breaches under the Data Protection Act / UK GDPR states 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. The Council also has a lawful duty to inform the individuals without undue delay if a breach is likely to result in high risk to their rights and freedoms.

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. This 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**

During 2020/21 33 incidents were reported. This is a significant increase on the previous year, suggesting that services are becoming more aware of the need to report incidents in a timely manner. Following assessment by the IG team one breach met the threshold for reporting to the ICO. The ICO reviewed the

Council's submission and did not recommend any further actions. A breakdown of all incidents 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 provided to the ISG to ensure visibility and ensure any recommendations 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, all 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.

10.3 Benchmarking against other public sector partners revealed that the recommended 2 yearly update was not in line with other areas of the public sector. This was identified as a risk to information sharing arrangements, especially for the sharing of health and social care data that was necessary as part of multi-agency Covid-19 work. As a result, the IG team recommended that all staff should undertake refresher training on an annual basis. This recommendation was agreed by ISG.

10.4 The IG Team provide quarterly updates on GDPR training completions to ISG. The Council has also procured a new e-learning platform which will remind staff when refresher training is due. This will be in place from 2021/22.

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.

(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, Numbers of internal reviews and ICO Complaints)

Appendix D	Breakdown of FOI Requests by Service Area (Percentage, Number of Requests, Compliance Levels)
Appendix E	Individual Rights Requests
Appendix F	Personal data incidents

16. BACKGROUND PAPERS

None

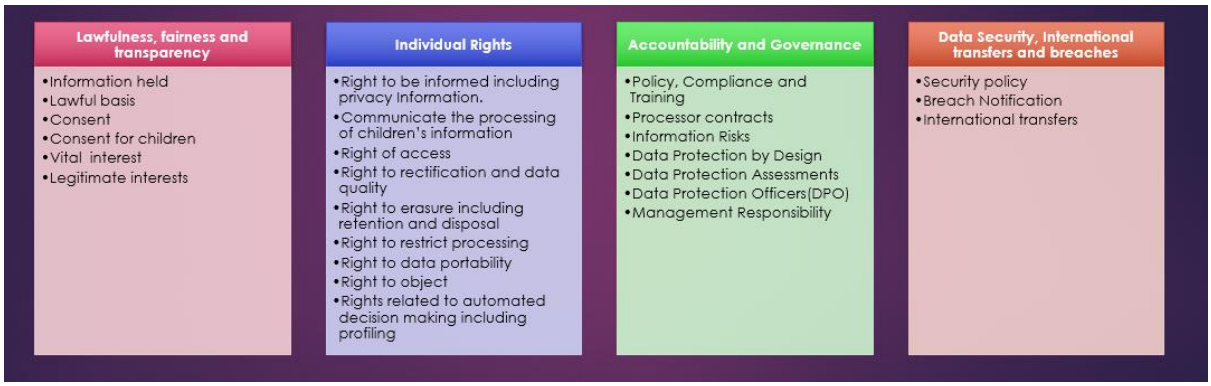
17. REPORT DETAILS AND CONTACT

Report: **Freedom of Information, Data Protection and Transparency: Annual Report 2019/2020**	Drafted: 28th July 2021 Last Revision: 28th July 2021
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:

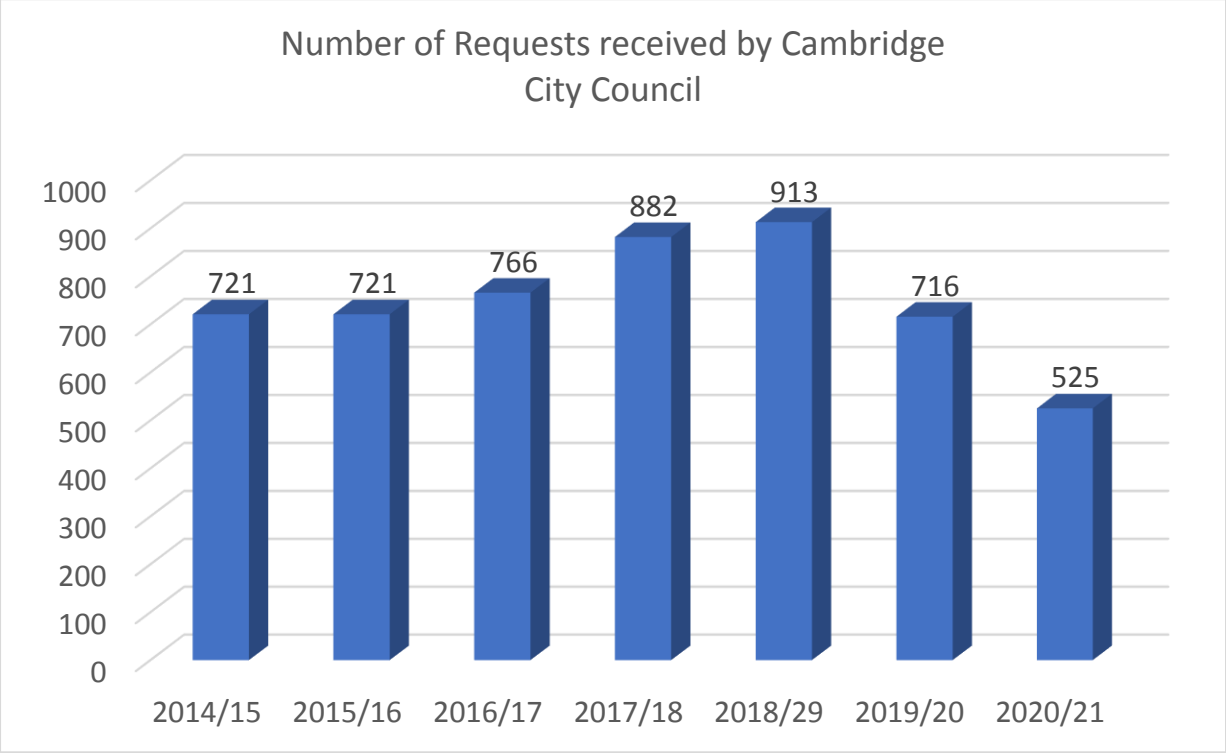
AREAS FOR MONITORING AND MANAGING CYBER SECURITY RISKS.

10 Steps Theme	Rating	RAG	Direction of travel
Risk Management *	7	GREEN	↑
Secure Configuration	7	GREEN	↔
Network Security	7	GREEN	↔
Managing user privileges	7	GREEN	↔
Incident management *	6	AMBER	↑
User education and awareness *	7	GREEN	↑
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	
2014/15	721	84	16	
2015/16	721	91	9	
2016/17	766	87	13	
2017/18	882	90	10	
2018/29	913	91	9	
2019/20	716	88	12	
2020/21	525	95	5	

c) FOI/EIR Complaints / Internal Reviews

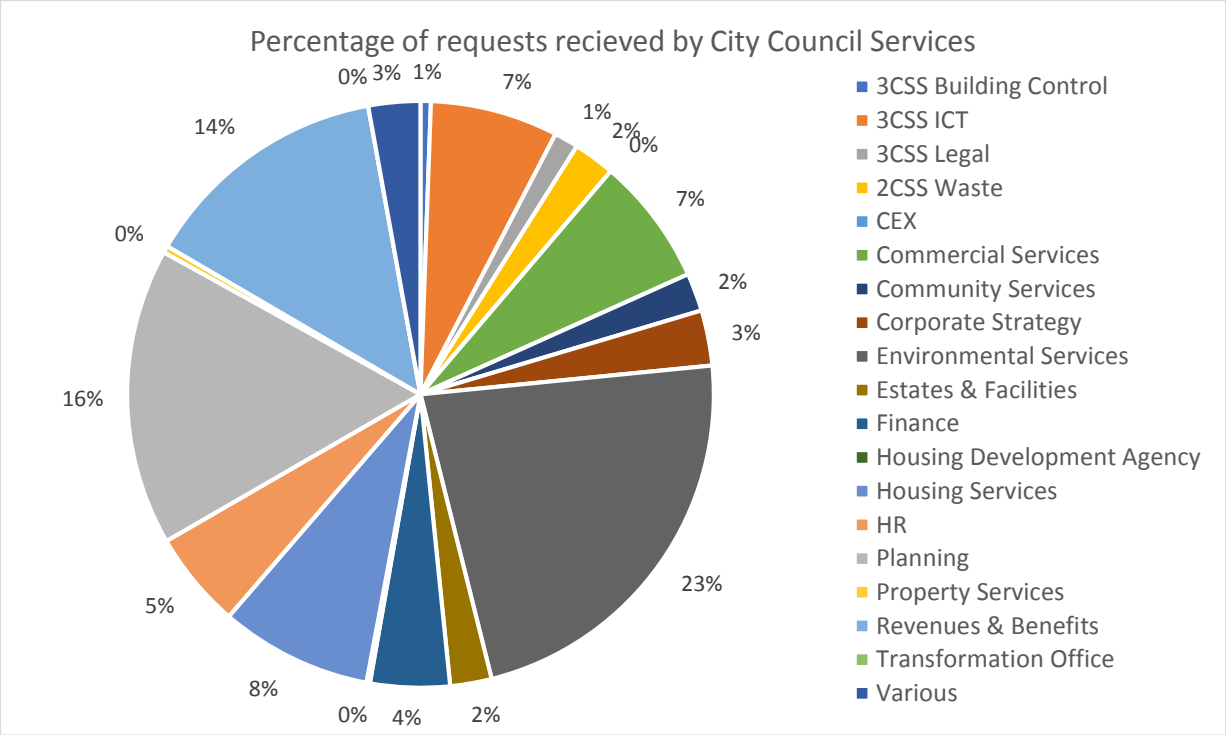
	Received	Compliance with time frame
Internal Reviews / Complaints	4	4
ICO Complaints	1	1

Whilst one complaint has been made to the regulator (ICO) it resulted in no action for the Council.

APPENDIX D:

BREAKDOWN OF FOI REQUESTS BY SERVICE AREAS

a) Percentage of Requests received by each Service Area



b) 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	3	3	100%	10.7
3CSS ICT	37	31	84%	15.5
3CSS Legal	7	7	100%	14.6
2CSS Waste	12	11	92%	14.8
CCC CEX	0	0	-	-
CCC Commercial Services	37	37	100%	5.2
CCC Community Services	11	11	100%	10.0
CCC Corporate Strategy	16	16	100%	12.3
CCC Environmental Services	119	118	99%	12.4
CCC Estates & Facilities	12	11	92%	16.3
CCC Finance	23	22	96%	17.3
CCC Housing Development Agency	1	1	100%	20.0
CCC Housing Services	44	44	100%	9.3
CCC HR	28	28	100%	14.2
CCC Planning	86	76	88%	13.2
CCC Property Services	2	2	100%	9.5
CCC Revenues & Benefits	72	66	92%	12.0
CCC Transformation Office	0	0	-	-
Various	15	13	87%	15.6
	525	**497**	**95%**	

APPENDIX E:

Individual Rights Requests

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

E.g. Subject Access, Erasure, and Rectification requests.

Other Requests	Received	Compliance with time frame
Individual Rights Requests (including SAR, erasure and rectification requests)	27	23
SAR Complaints	0	-
ICO Complaints	1	1

Whilst one complaint has been made to the regulator (ICO) it resulted in no further action for the Council.

APPENDIX F:

PERSONAL DATA INCIDENTS

Personal data incidents recorded in 2020/21 (April 2020 – Mar 2021) by Category.

Category	Number	Reported to ICO
Disclosed in error	24	Not reportable to ICO
Lost or stolen hardware	1	Not reportable to ICO
Uploaded to website in error	1	Not reportable to ICO
Technical security failing	1	Not reportable to ICO
Other	6	1
Total	33	1