FREEDOM OF INFORMATION, DATA PROTECTION AND TRANSPARENCY: ANNUAL REPORT 2021/2022

To: Civic Affairs Committee	**September 2022**
Report by:	**Kirsty Squires/Eleanor Dent** **Data Protection Officer & Information Governance Manager/ Deputy Data Protection Officer & Senior Information Governance Specialist** **(3C Shared Services - Information Governance)** **Email:** **Kirsty.Squires@3csharedservices.org** **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 2021/22 (April 2021 - March 2022).

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 the council's performance relating to:
  - Freedom of Information (FOI) Act / Environmental Information Regulations (EIR) Requests
  - Data Subject Access Requests
  - Personal Data Incidents

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. This includes access to information, data quality, information management, information security and information sharing, data privacy and data protection and other relevant information law compliance, including but not limited to the Freedom of Information Act, the Data Protection Act/UK GDPR, the Environmental Information Regulations, Privacy in Electronic Communications Regulations.

4. ORGANISATIONAL ARRANGEMENTS

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 post holder is 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. The three councils are currently considering moving to one joint Information Security and Governance Board.

4.5 The Information Security Group meets quarterly and last met in July 2022.

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 incoming DPO has produced a health check report to highlight areas of good practice and areas requiring development to move the council on with their compliance journey.

5.3 A priority action plan will be presented to the October Information Security Group meeting for agreement.

5.4 Updates to monitor the status and progress of these actions will be provided to the City's Information Security Group (ISG) or new Information Security and Governance Board structure if adopted.

6. INFORMATION SECURITY COMPLIANCE

6.1 Confidentiality, Integrity and Availability collectively form the security objectives for the council to protect the information and systems, providing assurances to residents, members of public and partner agencies.

6.2 As with previous years the council continue to invest time, effort, and resource into managing and mitigating cyber risks and threats. The creation of a dedicated cyber security post will support 3C ICT in maintaining the current cyber security posture.

6.3 With the ongoing conflict in Eastern Europe, 3C ICT has reviewed risks and implemented additional checks based on the National Cyber Security Centre (NCSC) recommendations. NCSC has warned all UK organisations to prepare for Russian cyber attacks

6.4 3C ICT and the Department for Levelling Up, Housing and Communities (DLUHC) are working together where a review of the mitigation in place to reduce cyber risk and the impact of malware and ransomware attacks has been completed. A

subsequent cyber treatment plan has been created and a grant awarded to improve mitigation.

6.5 3C ICT continue to maintain the statuses of the themes identified in the NCSC 10 Steps to Cyber Security. High profile incidents including the ransomware attack on Gloucester City Council in December 2021 continue to occur. The cyber treatment plan created with support from DLUHC will allow for the status for monitoring to move to green in Q3 this FY. See **Appendix A** for summary of themes and RAG status.

6.6 Last year it was reported that two areas were in amber. Although two are still amber, improvements have been made in each area. As reported last year 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 two areas is the following:

- Incident Management – Still regarded as amber, this area has improved with reviews and improvements made for the current reporting of and response to incident processes. 3C ICT are continuing to promote user awareness and the importance of reporting any incidents.
- Monitoring – Although this theme is still graded as amber, monitoring of the network for suspicious activity is done. Work to centralise all logging to a single solution is expected to be completed October 2022 and will allow this them to move to green.

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. **In 2021-22 we achieved 83%.**

This section of the report relates to those formally processed requests.

7.3 For the year 2021/22 (April – March) the council received a total of 627 requests under FOI and EIR, representing a 19% increase in the number of requests received in 2020/21 (525 requests).

7.4 **Appendix B** demonstrates the year on year trend in the number of FOI requests since 2014/2015 – 2020/2021.

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

The departments with largest number of requests are Commercial Services (65), Environmental Services (147) and Planning Services (65).

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. The most recent proposed amendment, The Data Protection Bill (which is due it's second reading on 5th September proposes further change to the regime around the management of personal data). 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 UK Data Protection Regulation. The regulation gives individuals specific rights over their information.

8.3 The Information Governance Team coordinate requests relating to individuals rights such as right of access to 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 D includes the performance data related to this area.

There were 44 (27 in 2020-21), representing a 63% increase requests made during the year, of which 12 (23 in 2020-21), were responded to within target date. Of the remaining 32 3 were classed as complex cases and as such had extended timescales. A further 22 were withdrawn/invalid.

8.4 5 rights requests were escalated to the Information Commissioner's Office.

9. PERSONAL DATA INCIDENTS /BREACHES

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 high risk to the rights and freedoms of individuals, the Council must inform the ICO within 72 hrs of becoming aware. 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 The IG team process is now well established and understood by council teams. When incidents are reported they are assessed to identify:

- 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.

9.3 The IG Team maintain 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 Incidents/Breaches**

During 2021/22 30 incidents were reported (33 in 2020-21) representing a decrease of 10% on the previous year. Following assessment by the IG team no incidents (1 last year) met the threshold for reporting to the ICO. 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. The majority of the incidents reported were where data had been shared with the incorrect recipient (mainly by email). A small number related to publication of personal data on the council 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. Lessons learned from other authorities and ICO cases in general

are also shared to reduce likelihood of occurrence of similar events within the council.

10 TRAINING

10.1 To ensure organisational compliance with the law and relevant guidance relating to Information Governance, all staff must receive appropriate and relevant training at regular intervals.

10.2 In 2020-21 it was recommended the council move to an annual mandatory refresher of GDPR and cyber security training, this recommendation was adopted.

10.3 The IG Team provide quarterly updates on GDPR training completions to 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.

(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	Areas for monitoring and managing cyber security risks
Appendix B	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 C	Breakdown of FOI Requests by Service Area (Percentage, Number of Requests, Compliance Levels)
Appendix D	Individual Rights Requests
Appendix E	Personal data incidents

16. BACKGROUND PAPERS

None

17. REPORT DETAILS AND CONTACT

Report: **Freedom of Information, Data Protection and Transparency: Annual Report 2021-22**	Drafted: 12/08/2022 Last Revision: 12/08/22
The author and contact officer for queries on the report	Information Governance Manager / Data Protection Officer infogov@3csharedservices.org

APPENDICES

APPENDIX A:

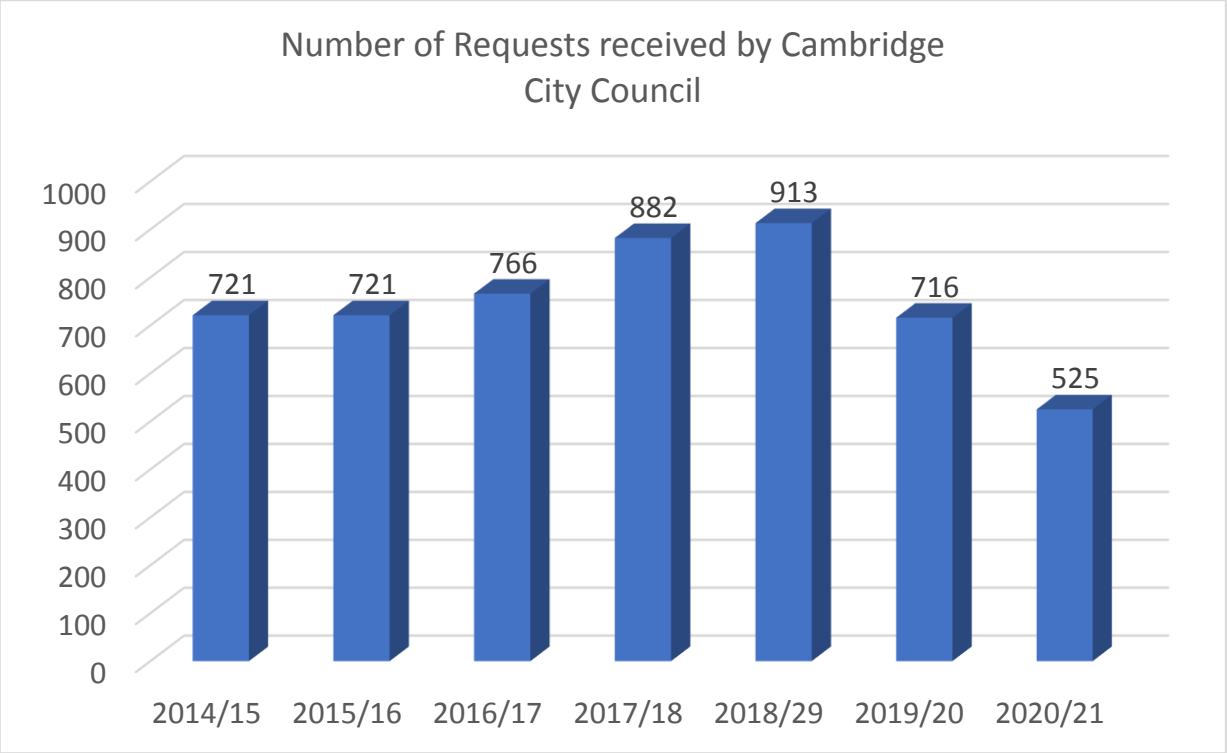
Q1 2022/23 AREAS FOR MONITORING AND MANAGING CYBER SECURITY RISKS.

10 Steps Theme	Rating	RAG	Direction of travel
Risk Management *	7	GREEN	⟷
Secure Configuration	8	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 B:

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 (%)
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
2020/21	525	95	5	90

c) FOI/EIR Complaints / Internal Reviews

	Received	Compliance with time frame
Internal Reviews / Complaints	7	6
ICO Complaints	5	4

APPENDIX C:

BREAKDOWN OF FOI REQUESTS BY SERVICE AREAS

a) Compliance level by each area

Service	Received	Response in 20 working days	% responded to in 20 working days	Average response time (working days)
2CSS Waste	8	8	100%	12
3CSS Building Control	3	3	100%	7
3CSS ICT	33	26	79%	6
3CSS Legal	1	0	0%	22
CCC Commercial Services	65	63	97%	7
CCC Community Services	8	7	86%	3
CCC Corporate Strategy	20	17	85%	9
CCC Environmental Services	147	117	79%	11
CCC Customer Services	2	2	100%	9
CCC Planning	65	56	86%	7
CCC Estates & Facilities	20	8	40%	26
CCC Finance	31	17	55%	16
CCC Housing Development Agency	2	1	50%	20
CCC Housing Services	49	42	86%	13
CCC HR	23	19	83%	15
CCC Property Services	4	4	100%	10
CCC Revenues & Benefits	37	30	81%	9
SCDC Environmental Services	10	10	100%	10
Other Authority	99	99	100%	3

APPENDIX D:

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)	44	12
SAR Complaints	1	-
ICO Complaints	5	4

APPENDIX E:

PERSONAL DATA INCIDENTS

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

Category	Number	Reported to ICO
Disclosed in error	26	0
Lost or stolen hardware	0	0
Uploaded to website in error	3	0
Technical security failing	1	0
Other	0	0
Total	30	0