REPORT TITLE: FREEDOM OF INFORMATION, DATA PROTECTION AND TRANSPARENCY: ANNUAL REPORT 2023-24

To:

Civic Affairs Committee 11th September 2024

Report by:
Adam Brown, Data Protection Officer & Information Governance Manager
Email: adam.brown@3csharedservices.org

Wards affected:
All

1. Recommendations

1.1 It is recommended that Civic Affairs Committee:

1. Note the contents of the report

2. Purpose and reason for the report

2.1 The purpose of this report is to provide an update on Information Governance activity and performance during 2023/24 (April 2023 - March 2024).

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 Act (FOIA) / Environmental Information Regulations (EIR) Requests
  - Data Subject Access Requests
  - Personal Data Incidents

3. Alternative options considered

3.1 This is an update report for members and so no alternative options considered at this stage.

4. Background and key issues

4.1 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.

Information Governance describes the comprehensive approach to managing information. This includes access to information, data quality, information management, information security and sharing, data privacy and data protection and other relevant information law compliance, including the Freedom of Information Act, the Data Protection Act/UK GDPR, the Environmental Information Regulations, and Privacy in Electronic Communications Regulations.

4.2 **ORGANISATIONAL ARRANGEMENTS**

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

The IG Team consists of six members:

- The Data Protection Officer (DPO)/Information Governance Manager, manages and oversees the service, and provides specialist advice on complex matters around data protection and information management for all three councils.
- The Deputy Data Protection Officer who provides cover and supports the team in the absence of the DPO and is also responsible for the information asset registers for the three councils and supports the Information Management Officers.
- The Requests Manager who leads the information requests and transparency functions for the team. The Requests Manager provides specialist advice and

guidance to staff and Members on FOIA and EIR. This is a new post as of June 2023.

- Information Management Officers who provide advice and guidance to the councils' internal departments on matters relating to data sharing, data protection impact assessment and personal data incident investigations.
- Two part time Information Governance Officers who manage incoming information requests and coordinate internal requests for support around personal data incidents/breaches, advice on data sharing and data protection impact assessments/contract reviews.

As this is a shared service, the Data Protection Officer (DPO) is the statutory DPO for all three authorities.

A Joint Information Governance and Security Board was established in April 2023, to replace Cambridge City Council's Information Security Group. The Board is made up of representatives of Cambridge City Council, HDC, and SCDC to ensure that the three councils work together to manage their data and to ensure good information security and governance. The Information Governance and Security Board monitors and is responsible for ensuring that the council meets the compliance obligations of relevant information law.

Terms of reference for the Joint Information and Security Board were agreed in April 2023.

The Joint Information Governance and Security Board meets quarterly and last met in July 2024.

4.3 DATA PROTECTION COMPLIANCE

Compliance against the obligations of the Data Protection Act and UK GDPR are monitored in line with the ICO's Accountability Framework.

The ICO's Accountability Framework has been expanded, where appropriate, to consider the other information law regimes that come under the remit of the 3C ICT Information Governance service which are.

- Freedom of Information Act (FOIA), and
- Environmental Information Regulations (EIR).

The Information Governance Team work against identified risks and issues in the Accountability Framework, against the areas of

- Contracts and Data Sharing
- Individual's Rights
- Leadership and Oversight
- Policies and Procedures
- Risk and DPIA
- Lawful Basis and Records of Processing Activity (ROPA)

- Training and Awareness
- Transparency

Updates to monitor the status and progress of the plan are provided to the Joint Information Governance and Security Board on a quarterly basis.

New guidance and policies introduced in 2023-24 include.

- Data Protection Policy
- Appropriate Policy Document
- Access to Information Policy
- Acceptable Use Policy
- Generative AI Policy, and AI guidance microsite for staff
- Record Retention and Management Policy

4.4 INFORMATION SECURITY COMPLIANCE

Cybersecurity continues to be crucial to daily operations and standard corporate procedures. The council must maintain safe and secure systems that give residents, members of the public, and partner agencies assurance to integrate systems and share information and data across numerous platforms.

3C ICT are still working with The Ministry of Housing, Communities and Local Government (MHCLG) to lower cyber risk. The internal vulnerability scanning solution has been set up. This has enabled the security team to focus on fixing issues based on risk score.

As a result of setting up and configuring systems that help to safeguard and oversee the environment, the council decided to finance an additional role in the cyber team. The team expansion was driven by the MHCLG recommendations of the need for these systems.

The National Cyber Security 10 Steps have maintained green status throughout the year. User education enhancements were the priority, with quarterly phishing test campaigns initiated in the last quarter. The outcomes of the test identified staff that required additional help in how to identify phishing emails.

Changes to the endpoint detection and response solution has enhanced the council's security posture as it provides continuous and comprehensive visibility into what is happening on endpoints in real time.

4.5 DATA PROTECTION REQUEST PERFORMANCE

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

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.

Individuals' rights requests must be responded to within a month.

Individual requests made during the year were as follows:

	Received	Compliance with time limit
Data Rights Requests (including Erasure Requests, etc.)	21	90%
SAR Reviews	3	67%
ICO SAR Complaints	0	-

Table 1: Personal information rights requests 2023-24

Whilst not required by the Data Protection Act, it is best practice to provide a review stage to personal information rights requests. As with requests made under FOIA or EIR this allows the Council the opportunity to review its handling of the request and to consider any appeals that the requester has made in relation to their request.

Requesters also have a right to complaint to the ICO in their capacity as the regulator. The Council did not receive any complaints from the regulator this year.

4.6 PERSONAL DATA INCIDENTS AND BREACHES

The guidance on notification of data breaches under the Data Protection Act / GDPR is that if an incident is likely to result in high risk to the rights and freedoms of individuals, the Council must inform the ICO within 72 hours of becoming aware of the issue. 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.

As result, the Information Governance 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.

The assessment is conducted by a member of the IG team when an incident is logged by a Service Area.

All incidents relating to personal data are logged to identify any trends, with the view to establish if any specific mitigations need to be put into place to prevent likely recurrence. Mitigations include requiring additional training, reviewing current processes, or issuing advice or briefing notes.

	Incidents/breaches	Reported to ICO
2020-21	32	1
2021-22	29	1
2022-23	26	1
2023-24	35	1

Table 2: Personal data incidents 2020-2024

35 incidents were reported and investigated in 2023-24. Of these, one incident was considered to meet the threshold for reporting to the ICO.

The ICO reviewed the incident and confirmed the findings of the investigation. The ICO closed the case with no further actions for the Council.

A breakdown of all incidents is as follows:

Type of Incident (Category)	Number
Personal details inappropriately disclosed (e.g. via email or by post)	20
Lost or stolen paperwork	5
Technical security failure	4
Uploaded to website in error	2

Lost or stolen equipment	1
Unauthorised access/disclosure	1
Other	2

Table 3: Categories of personal data incidents 2023-24

In all instances, immediate steps were taken by officers to mitigate the incident, once known. Examples of incidents include correspondence being sent to the incorrect recipient, or documents being inadvertently published to the website. All Council devices are remotely wiped once a loss or theft is reported, and usage logs checked to identify whether the device has been accessed following its loss.

A quarterly update on incidents is provided to the SIRO to ensure visibility and ensure any improvements needed are discussed and followed through as appropriate. Where relevant learning from breaches/incidents/near misses is also shared across the three councils to minimise the risk of further occurrence.

4.7 FREEDOM OF INFORMATION / ENVIRONMENTAL INFORMATION 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 (FOIA) works alongside the Environmental Information Regulations (EIR).

Requests for information that are not dealt with as part of the day-to-day business of the Council should be considered as Freedom of Information requests.

In October 2023 a new request management system for information requests was introduced. This system manages requests made under FOI, EIR and Data Protection requests.

3C ICT Information Governance oversees a request management system for handling information requests. Ownership of the response to these requests is placed on service areas by means of key responders and champions being designated and responsible for ensuring their service responds within the legal time limit of 20 working days. An Information Governance Officer coordinates all formal requests and allocates specialist support from the Information Governance team where service areas require this.

In 2023-24 (Apr – Mar) the council received a total of 623 requests under FOIA and EIR.

This represents a 9% increase in the number of requests received in the previous year. This brings the number of requests closer to the levels the Council received in 2019-20.

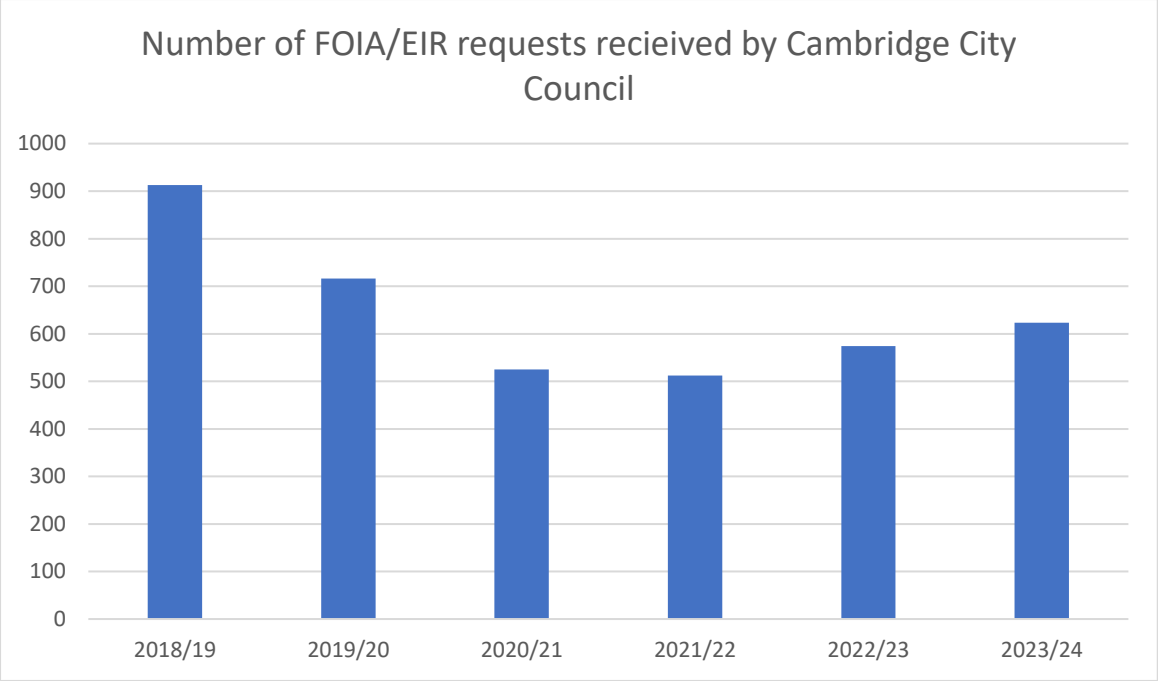

Chart 1: Information requests to Cambridge City Council 2018-2024

The Council works to a target of 90% response compliance within 20 days as advised by the Information Commissioner. The Council achieved 84% in 2023-24 which is a decline in performance from 89% last year.

Detail of the requests received across all Council services is provided below. The Communities Group received the most cases.

Service	Received
2CSS WASTE	8
3CSS Building Control	1
3CSS ICT	38
3CSS Legal	5
Greater Cambridge Shared Planning	50
Chief Executive Office	36
City Services	84
Communities Group	219
Corporate Group	166
Place Group	13
Various	3

Table 4: Number of requests per service area

Access to information acts such as FOIA and EIR provide a limited right of access. Information may be withheld if an exemption applies to its disclosure. All the information was provided for most requests with 72% of requests receiving a full or partial response. See breakdown of outcomes below.

Request Outcome	Count
All information provided	365
Some information provided; remainder exempt	47
Some information provided; remainder not held	11
Not held	97
Refused on grounds of time/cost	3
Exemptions applied to all information	46
Concluded outside of legislation	1
Withdrawn	29
Vexatious	1

Table 5: Outcomes to information requests 2023-24

The IG team continue to provide reports on performance and compliance with the legislation, which are shared on the City Council intranet on a quarterly basis. These reports also enable services to understand trends, and to help focus on what should be uploaded onto their publication scheme.

Requestors have the right to a review of their case if they are not satisfied with the outcome or how the request was handled, before taking further action to the Information Commissioner's Office.

	Received	Response within 20 working days
Internal Reviews	11	91%
ICO Complaints	2	100%

Table 6: Information request reviews and complaints to regulator 2023-24

Two cases were investigated by the regulator. The regulator upheld the complaint of the requester in one case (IC-244144-N7D5), and issued a decision notice requiring further information to be released to the requester. The regulator upheld the position of the council in the second case (IC-270963-D7N4) and no further action was required.

4.8 **TRAINING**

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.

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

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

5. Corporate plan

5.1 The report provides assurance that the Council is meeting it's strategic priorities under **Priority 4: Modernising the council to lead a greener city that is fair for all** by running our services in an efficient way and continuously improving our services

6. Consultation, engagement and communication

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

7. Anticipated outcomes, benefits or impact

7.1 The Council takes transparency issues seriously and is broadly compliant with the legislation. Several measures have been put into 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.

8. Implications

8.1 Relevant risks

No decision required that would result in impact to risks

Financial Implications

8.2 No decisions with financial implications are proposed in this report.

Legal Implications

8.3 No decisions with legal implications are proposed in this report

Equalities and socio-economic Implications

8.4 This report does not propose decisions with equalities impacts, so an EqIA has not been produced.

Net Zero Carbon, Climate Change and Environmental implications

8.5 No decisions with environmental implications are proposed in this report.

Procurement Implications

8.6 Not Applicable

Community Safety Implications

8.7 Not Applicable

9. Background documents

Used to prepare this report, in accordance with the Local Government (Access to Information) Act 1985

9.1 There are none