# REPORT TITLE: Annual Information Governance and Cyber Security Report 2024-25

**To:**
Civic Affairs and Audit Committee (date tbc)

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

**Wards affected:**
All

Director Approval: Director Jane Wilson confirms that the report author has sought the advice of all appropriate colleagues and given due regard to that advice; that the equalities impacts and other implications of the recommended decisions have been assessed and accurately presented in the report; and that they are content for the report to be put to the Committee.

## 1. Recommendations

1.1 It is recommended that Civic Affairs and Audit Committee note the contents of this 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 2024/25 (April 2024 – March 2025).

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

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

## 4. Background

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.

### 4.1 Organisational arrangements

The Information Governance 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 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.
- Information Management Officers who support the Information Governance Officers with complex information requests and 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. The Board is made up of representatives of HDC, SCDC and Cambridge City Councils to ensure that the three councils work together to ensure good information security and governance. The Joint 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 reviewed and agreed in October 2024.

The Joint Information Governance and Security Board meets quarterly and last met in October 2025.

## 4.2 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 main 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.

There have been no new policies introduced this year with all previous outstanding policies for Information Governance and Security now up to date and within a review cycle. Work is now ongoing to align policies to a standardised policy framework for Information Security

New policies reviewed in 2024-25

- Generative AI Policy
- Internal Review Policy
- Information Governance Framework
- Information Management Policy

- Information Security Policy

## 4.3 Information Security Compliance

Cyber security remains vital for everyday operations and regular business processes. The council must keep systems that are secure and reliable, so that residents, public users, and partner agencies can trust them to connect systems and share information and data across various platforms.

Following from recommendations from the Department for Levelling Up, Housing and Communities (DLUHC) last year the Cyber and Information Security Team have expanded and taken on a new member of staff. This, along with additional measures such as continuous vulnerability management, and a focus on vulnerability patching have improved the cyber security posture of the Council.

The approach of the Cyber and Information Security Team is to follow the principles of the NCSC Cyber Assessment Framework (CAF) and 10 Steps to Cyber Security. The service reports into the Joint Information and Security Board on a quarterly basis, with a detailed report against high and medium cyber security risks.

The Joint Information and Security Board also receive a quarterly report on cyber security incidents. The number and cause of incidents are given in the table below.

| Cause of incident | Number of incidents |
|---|---|
| Malware | 1 |
| Anti-virus disabled | 1 |
| Supply chain phishing | 1 |

Table 1: Cyber security incidents 2024-25

In each case action was taken to contain the incident and additional monitoring was applied to affected accounts and devices to provide assurance that no malicious activity has occurred. In the case of anti-virus being disabled this was identified due to additional controls being put in place by the Cyber and Information Security Team.

**Simulated Phishing Campaigns.**

Phishing is the practice of sending emails that appear to be from a reputable source but are sent by a malicious actor. It is estimated that around 80% of all security incidents start with email-based phishing, and due to the success of this strategy, the number and sophistication of these attacks is rapidly increasing.

In order to gain visibility into the risk specific to the council, raise user awareness, and improve user capability to detect and appropriately handle Phishing emails, 3C ICT use “Simulated Phishing Campaigns” which involves sending realistic but safe Phishing emails to users on a regular basis. These campaigns have been running over the course of 2024-25, and the results reported to the Joint Information and Security Board.

Over the course of 2024-25 user awareness has improved, as evidenced by a decrease in the number of phishing e mails that have been opened, as well as an increase in the number reported. Remedial training is targeted at those staff who engage with these e mails.

Simulated phishing exercises are only one of several mitigations the Council has in place to reduce the risk posed by phishing, including e mail security, antivirus and firewalls.

## 4.4 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.

Individual rights requests must be responded to within a month. Individual requests made during the year were as follows:

| Category | Received | Compliance with time frame (30 Days) |
|---|---|---|
| Data Rights Requests (including SAR, erasure and rectification requests) | 34 | 88% |
| SAR Complaints | 0 | - |
| Disclosure for Crime and taxation purposes | 20 | 95% |
| Disclosure for Legal purposes | 6 | 66% |

Table 2: Data Protection requests 2024-25

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. The Council had no complaints relating to Data Protection Rights this year.

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

## 4.5 Personal data incidents and breaches

The guidance on notification of data breaches under the Data Protection Act / GDPR is that if a breach or 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 carried out by a member of the Information Governance team when an incident is reported by a Service Area.

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

| | Incidents/breaches | Reported to ICO |
|---|---:|---:|
| 2020-21 | 11 | 0 |
| 2021-22 | 25 | 2 |
| 2022-23 | 27 | 0 |
| 2023-24 | 20 | 1 |
| 2024-25 | 46 | 0 |

Table 3: Personal data incidents 2020-2025

46 incidents were reported in 2024-25, an increase in the number of incidents from last year. The volume of these incidents without a report to the Information Commissioners Office evidence a promising trend of increased reporting of low level breaches. A breakdown of these is as follows:

| Type of Incident (Category) | Number |
|---|---:|
| Disclosed in error | 34 |
| Lost or stolen paperwork | 2 |
| Technical security failure | 5 |
| Uploaded to website in error | 1 |
| Unauthorised access/disclosure | 4 |

Table 4: Categories of personal data incidents 2024-25

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.

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.

The information Governance Team have published a series of guidance documents, including a number of data protection topics as well as how to identify and report a data breach this year. Additional training and support are also provided to services where repeat incidents occur identify and eliminate root causes of these incidents.

### 4.6 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.

3C ICT Information Governance oversees the 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 timeframe 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 2024-25 (Apr – Mar) the council received a total of 615 requests under FOIA and EIR. This represents a 1.4% increase in the number of requests received on the previous year.

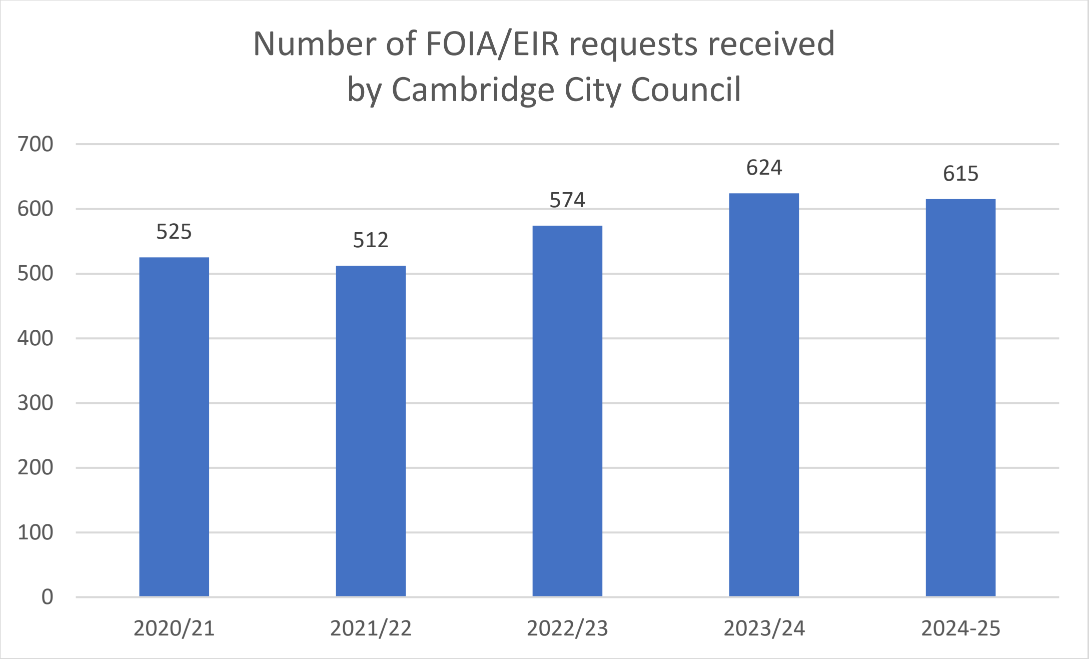

Chart 1: FOIA and EIR requests received by CCC 2020-25

The Council works to a target of 90% response compliance within 20 days as advised by the Information Commissioner. The Council achieved 86% in 2024-25 which is an improvement of 5% on the response rate of 2023-24.

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

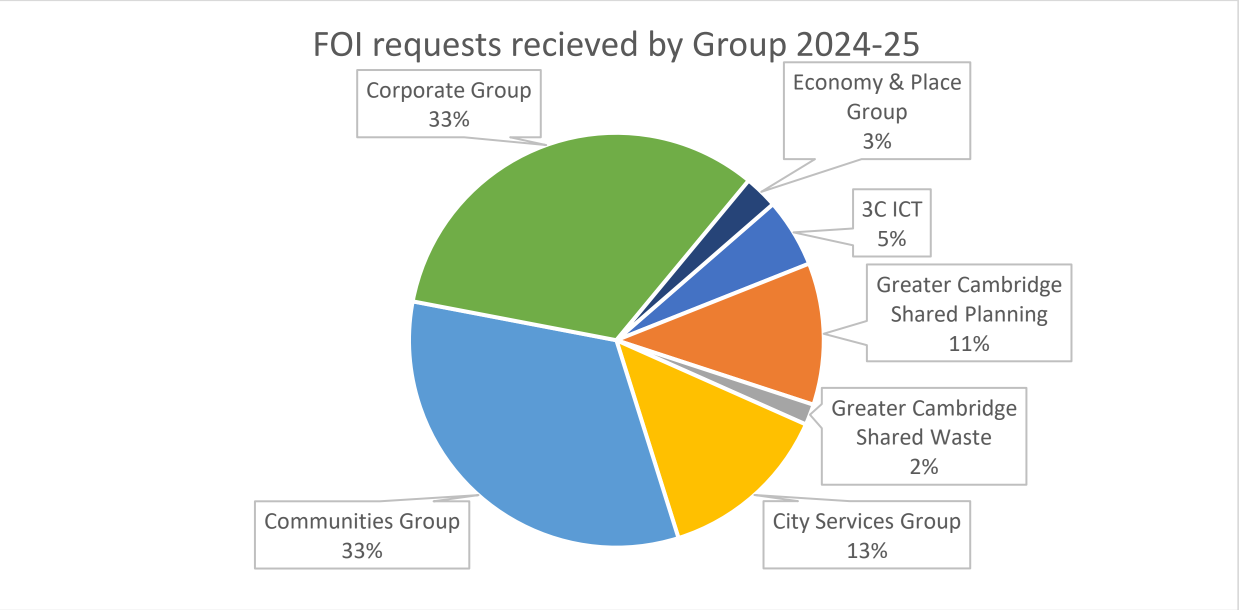

Chart 2: FOI requests by Group

Access to information acts such as FOIA and EIR provide a limited right of access. Some information may be withheld if an exemption to disclosure applies. All requested information was provided in most cases, with information being exempted in only 18% of cases. See breakdown of outcomes below.

| Request Outcome | Count |
|---|---|
| All information provided | 380 |
| Some information provided; remainder exempt | 51 |
| Some information provided; remainder not held | 3 |
| Exemptions applied to all information | 64 |
| Exceeds reasonable limits | 4 |
| Not held | 59 |
| Withdrawn | 55 |

Table 5: Outcomes to information requests 2024-25

The Information Governance team continue to provide reports on performance and compliance with the legislation, which are shared on the Cambridge 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 | 8 | 100% |
| ICO Complaints | 2 | Both still open pending ICO investigation |

Table 6: Information request reviews and complaints to regulator 2024-25

### 4.7 Looking Forward

The team have ambitious goals moving forward, with a number of these being delivered alongside colleagues in ICT. Primarily working towards adherence to standardised Policy and Risk Frameworks for Information Security.

Building on this in the next year the team is looking to implement more technical controls around management and security of data based on the organisational controls already in place.

## 5. Corporate plan

5.1 Information Governance and Cyber Security support the Council's overarching vision of "One Cambridge – Fair for All" in the following ways.

- **Cyber security and resilience** protect the infrastructure that supports inclusive digital services.
- **Data protection compliance** ensures fair use of data in service delivery and community engagement.
- **Transparency** fosters democratic accountability and empowers residents to participate in shaping their city.

## 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* *No decisions with procurement implications are proposed in this report.*

### Community Safety Implications

8.7 *No decisions with community safety implications are proposed in this report.*

## 9. Background documents

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

9.1 *There are none*