HUNTINGDONSHIRE DISTRICT COUNCIL

Title/Subject Matter: Annual Report on HDC Compliance with the Information Rights Acts (Freedom of Information Act, Environmental Information Regulations and UK GDPR) and Information Governance

Meeting/Date: Corporate Governance Committee - 24 September 2025

Executive Portfolio: Executive Councillor for Resident Services and Corporate Performance

Report by: Information Governance Manager & Data Protection Officer

Ward(s) affected: All Ward(s)

Executive Summary:

The Information Governance Service for Huntingdonshire District Council (HDC) is currently provided by 3C ICT Shared Service hosted by Huntingdonshire District Council. This also serves South Cambridgeshire District Council and Cambridge City Council.

The Information Governance (IG) Team leads on:

- data protection compliance advice,
- information and records management advice, and
- information requests under the Freedom of Information Act 2000, (FOIA) the Environmental Information Regulations (EIR) the Data Protection Act 2018 and the UK GDPR.

The team is led by the Information Governance Manager who is also the Data Protection Officer for the three councils.

This is an annual report on the Council's compliance with the Freedom of Information Act 2000 and Environmental Information Regulations 2004.

This report also includes the Councils performance regarding protecting personal data and covers the period April 2024 to March 2025.

The number of requests received by the Council in 2024-25 was 520; a decrease on the previous year's total of 642 (a 19% decrease).

Recommendation(s):

Corporate Governance Committee is asked to note the contents of this report.

1. PURPOSE OF THE REPORT

1.1 The purpose of this report is to provide an update on Information Governance activity and performance during 2024-25; and highlight any issues encountered and actions to be undertaken to improve performance.

1.2 It provides:

- An overview of the current arrangements in place to monitor the Information Governance at the Council including Data Protection Compliance and Information Security / Cyber Security Compliance.
- An update on performance relating to:
  - Freedom of Information Act (FOIA) / Environmental Information Regulations (EIR) Requests
  - Data Subject Rights Requests
  - Personal Data Breaches

2. BACKGROUND

2.1 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. This aligns with Priority 3 of the Corporate Plan, Delivering good-quality, high value-for-money services with good control and compliance with statutory obligations.

2.2 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

3. ORGANISATIONAL ARRANGEMENTS

3.1 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 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.

3.2 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 also 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.

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

3.4 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.

3.5 Terms of reference for the Joint Information and Security Board were reviewed and agreed in October 2024.

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

4. DATA PROTECTION COMPLIANCE

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

4.2 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).

4.3 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

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

4.5 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

4.6 Policies reviewed in 2024-25

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

5. INFORMATION SECURITY COMPLIANCE

5.1 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.

5.2 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.

5.3 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.

5.4 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

5.5 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.

5.6 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.

5.7 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.

5.8 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.

5.9 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.

6. DATA PROTECTION – REQUEST PERFORMANCE

6.1 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.

6.2 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.

6.3 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)	28	20
SAR Complaints	1	1
Disclosure for Crime and taxation purposes	19	19
Disclosure for Legal purposes	1	1

Table 2: Data Protection requests 2024-25

6.4 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 one complaint relating to Data Protection Rights this year.

6.5 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.

7. PERSONAL DATA INCIDENTS AND BREACHES

7.1 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.

7.2 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.

7.3 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	30	1

Table 3: Personal data incidents 2020-2025

7.4 30 incidents were reported in 2024-25, an increase in the number of incidents from last year. A breakdown of these is as follows:

Type of Incident (Category)	Number
Personal details inappropriately disclosed (e.g. via email or post)	27
Lost or stolen hardware	1
Unauthorised access or disclosure	1
Uploaded to website in error	1

Table 4: Categories of personal data incidents 2024-25

7.5 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.

7.6 One incident in 2024-25 was assessed to be of a severity to report to the Information Commissioner's Office (ICO). The Information Governance team worked with the affected service to review the circumstances of the incident, and to identify mitigating actions to be taken by the service to prevent a similar breach occurring in the future. The ICO did not take any further action against the Council and has closed the case.

7.7 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.

7.8 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.

8. FREEDOM OF INFORMATION / ENVIRONMENTAL INFORMATION REQUESTS

8.1 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).

8.2 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.

8.3 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.

8.4 In 2024-25 (Apr – Mar) the council received a total of 520 requests under FOIA and EIR. This represents a 19% decrease in the number of requests received in the previous year and is close to the number of requests received in 2020.

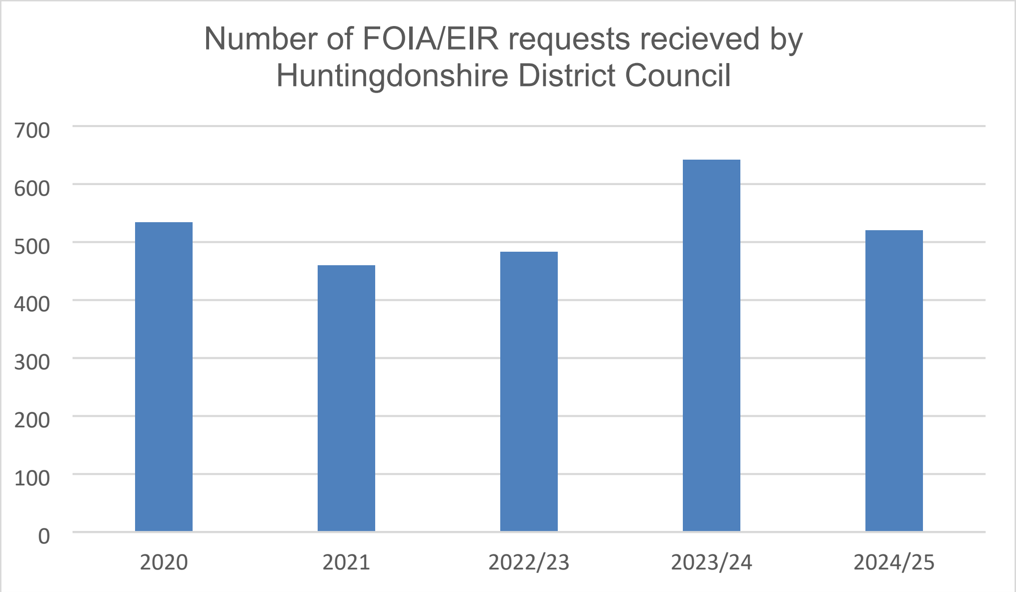

Chart 1: FOIA and EIR requests received by HDC 2020-25

8.5 The Council works to a target of 90% response compliance within 20 days as advised by the Information Commissioner. We achieved 81% in 2024-25 which is the same response rate as the previous year.

8.6 Detail of the requests received across all Council services is provided below. The Chief Operating Officer services and Community Services have received the most cases.

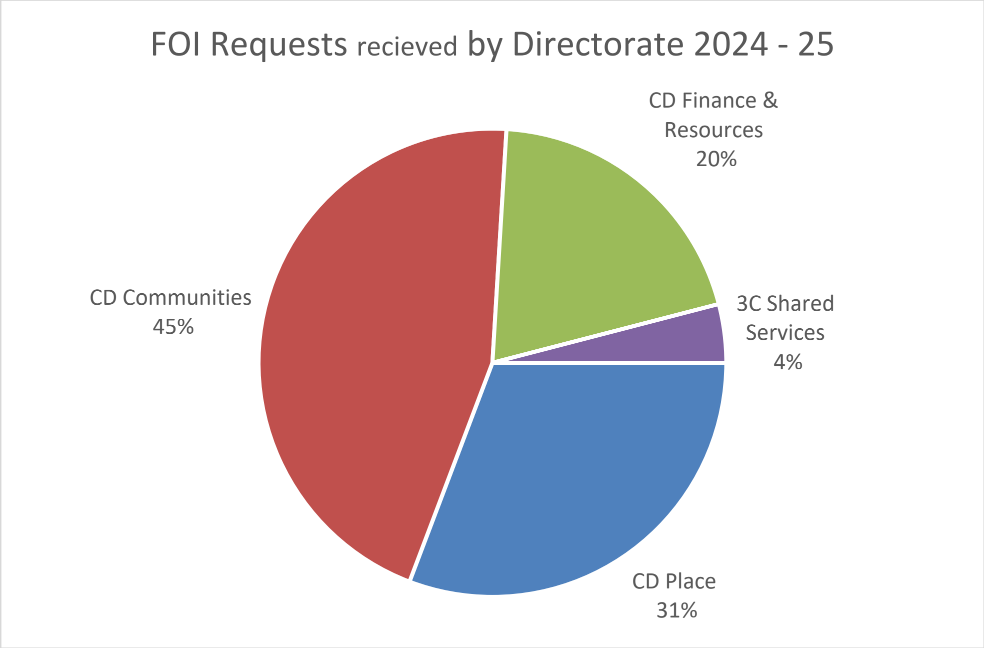

Chart 2: FOI requests by Directorate

8.7 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 14% of cases. See breakdown of outcomes below.

Request Outcome	Count
All information provided	329
Some information provided; remainder exempt	7
Some information provided; remainder not held	11
Exemptions applied to all information	67
Exceeds reasonable limits	3
Not held	55
Withdrawn	46

Table 5: Outcomes to information requests 2024-25

8.8 The Information Governance team continue to provide reports on performance and compliance with the legislation, which are shared on the HDC 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.

8.9 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	5	5
ICO Complaints	0	0

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

9. LOOKING FORWARD

9.1 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.

9.2 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.

CONTACT OFFICER

Name/Job Title:	Adam Brown, Data Protection Officer & Information Governance Manager
Email:	Adam.Brown@3csharedservices.org