Insert:
Corporate Governance Committee – 18th November 2026

Report by: Information Governance Manager & Data Protection Officer

Lead Cllr: N Hunt
Executive Councillor for Resident Services and Corporate Performance

Wards	Open / Exempt	Key Decision?
All Wards	Open	~~Yes /~~ No

2025/26 Compliance with Information Rights and Information Governance

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.

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 2025 to March 2026.

The number of requests received by the Council in 2025-26 was 563; an increase on the previous year's total of 520 (an 8% increase).

Recommendations

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

	Key Corporate Plan Priorities
1	***Delivering good quality, high value-for-money services with good control and compliance with statutory obligations***
2	

	Place Strategy Priorities
1	
2	

Report Author(s)

Adam Brown, Information Governance Manager & Data Protection Officer (adam.brown@3csharedservices.org)

1. PURPOSE OF THE REPORT

1.1 The purpose of this report is to provide an update on Information Governance activity and performance during 2025-26; 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.

1.3 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 & CONTEXT

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

2.3 Organisational Arrangements

2.3.1 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.

2.3.2 The Information Governance Team consists of eight 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.

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

2.3.4 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.

2.3.5 Terms of reference for the Joint Information and Security Board were reviewed and agreed in July 2026.

2.3.6 The Joint Information Governance and Security Board meets quarterly and last met in October 2026.

2.4 Data Protection Compliance

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

2.4.2 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)

2.4.3 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

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

2.4.5 Work has been ongoing to align policies to a standard framework which has resulted in 2 new policies and a significant number of policies in final draft at the end of the financial year

2.4.6 Policies reviewed in 2025-26

- Generative AI Policy
- Clear Desk Policy
- Patching Policy
- Incident Management Policy
- Database Administration Policy
- Data Protection Policy
- Access to Information Policy
- Retention Policy
- Appropriate Policy Document

2.5 Information Security Compliance

2.5.1 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.

2.5.2 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.

2.5.3 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 2025-26

2.5.4 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.

2.5.5 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

2.5.6 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 2025-26, and the results reported to the Joint Information and Security Board.

2.5.7 Over the course of 2025-26 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.

2.5.8 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

2.6 Data Protection – Request Performance

2.6.1 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.

2.6.2 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.

2.6.3 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)	23	74%
SAR Complaints	1	100%
Disclosure for Crime and taxation purposes	23	100%
Disclosure for Legal purposes	7	86%

Table 2: Data Protection requests 2025-26

2.6.4 The Data (Use and Access) Act 2025 introduced a statutory obligation to maintain an internal data protection complaints process. Prior to the implementation of the Act, it was considered best practice to provide a review stage to personal information rights requests, and the Council has included these in its Internal Review Policy since 2022. 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.

2.6.5 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.

2.7 PERSONAL DATA INCIDENTS AND BREACHES

2.7.1 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.

2.7.2 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.

2.7.3 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.
The Information Governance Team continues to encourage reporting of incidents to support learning and early identification of trends, and the increase of incidents is a result of increased awareness, ease of reporting and a continued effort to improve the culture of learning from incidents

	Incidents	Reported to ICO
2021-22	25	2
2022-23	27	0
2023-24	20	1
2024-25	30	1
2025-26	42	1

Table 3: Personal data incidents 2021-2026

2.7.4 42 incidents were reported in 2025-26, an increase in the number of incidents from last year. All reported incidents are reviewed and a breakdown of these follows:

Type of Incident (Category)	Number
Personal details inappropriately disclosed (e.g. via email or post)	28
Unauthorised access or disclosure	1
Near miss/Not a data breach	13

Table 4: Categories of personal data incidents 2025-26

2.7.5 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.

2.7.6 One incident in 2025-26 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 has not contacted the Council about any further action to date.

2.7.7 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.

2.7.8 The Information Governance Team deliver training and provide additional support for services where repeat incidents occur or following a high-risk data breach. This training and support are provided to identify and eliminate root causes of these incidents.

2.8 FREEDOM OF INFORMATION / ENVIRONMENTAL INFORMATION REQUESTS

2.8.1 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).

2.8.2 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.

2.8.3 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.

2.8.4 In 2025-26 (Apr – Mar) the council received a total of 563 requests under FOIA and EIR. This represents an 8% increase in the number of requests received in the previous year.

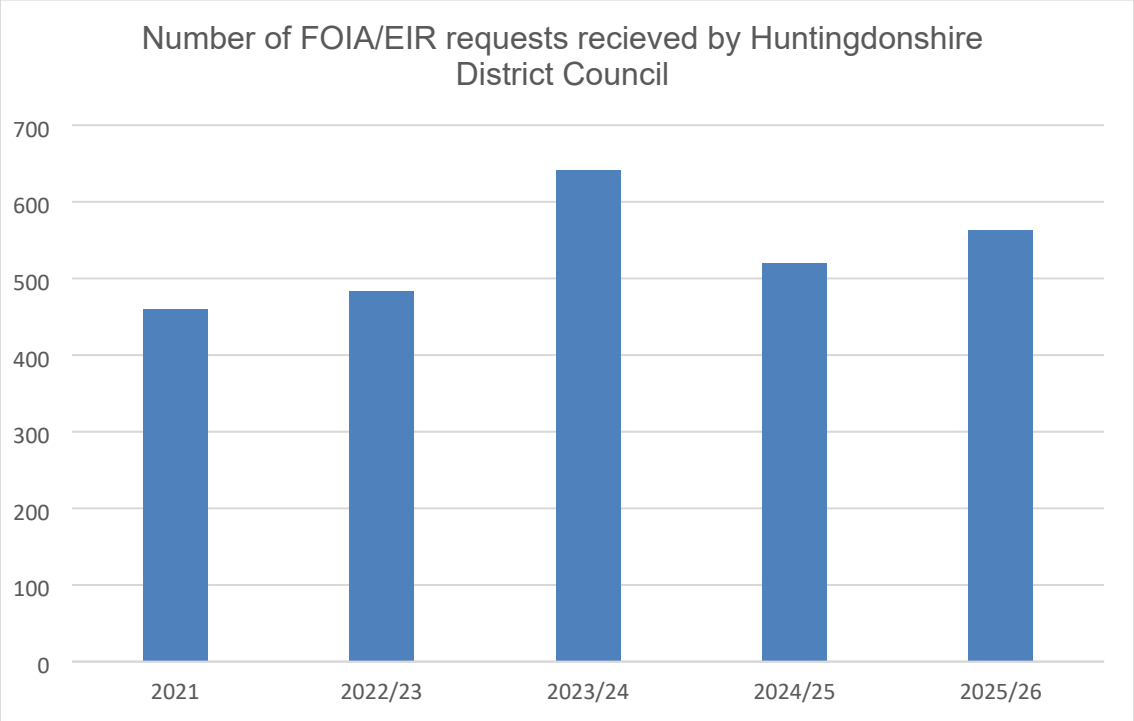


Chart 1: FOIA and EIR requests received by HDC 2021-26

2.8.5 The Council works to a target of 90% response compliance within 20 days as advised by the Information Commissioner. We achieved 86% in 2025-26 which is an improvement in the response rate from previous years, and the highest for six years.

2.8.6 Detail of the requests received across all Council services is provided below. The Place and Communities Directorates have received the most cases.

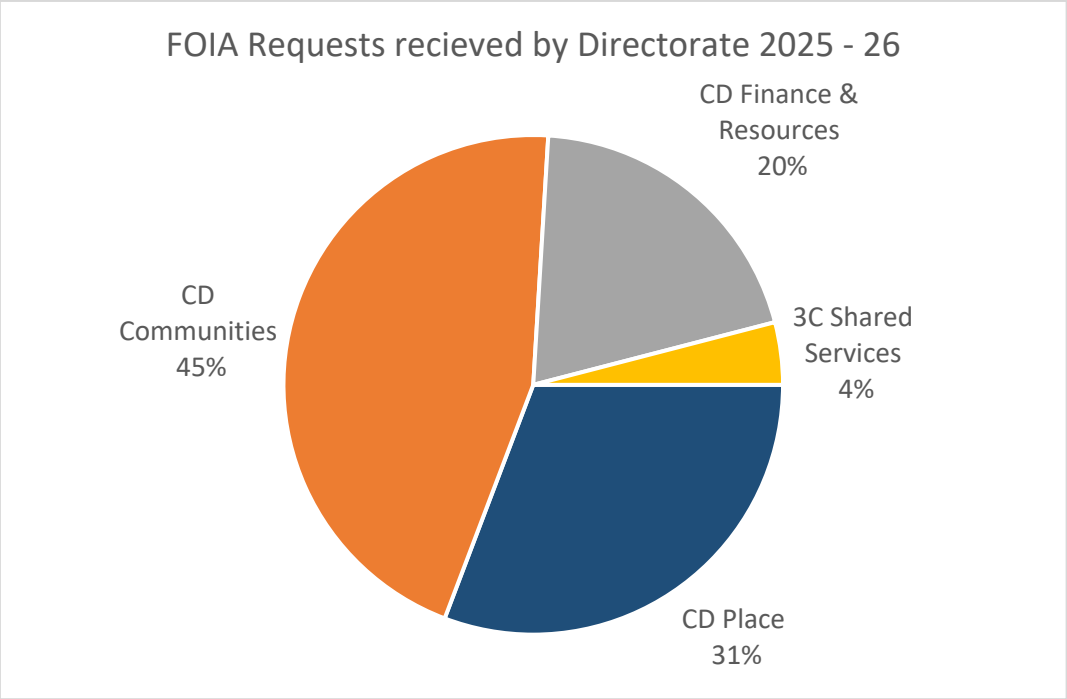


Chart 2: FOI requests by Directorate

2.8.7 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 13% of cases. See breakdown of outcomes below.

Request Outcome	Count
All information provided	365
Some information provided; remainder exempt	40
Some information provided; remainder not held	3
Exemptions applied to all information	72
Exceeds reasonable limits	4
Not held	51
Withdrawn	28

Table 5: Outcomes to information requests 2025-26

2.8.8 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.

2.8.9 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	15	93%
ICO Complaints	1	100%

Table 6: Information request reviews and complaints to regulator 2025-26

2.8.10 The ICO issued one decision notice relating to an information request received in January 2026. The request was responded to later than the statutory time frame, but before the decision notice was issued in June 2026.

2.9 LOOKING FORWARD

2.9.1 The team continue historical progress on service improvements, with a number of projects being run by the Information Governance team to continue to safeguard data and improve the compliance position of the council.

2.9.2 The Data Protection audit undertaken in January 2026 continues to provide headline direction for improvements to address gaps in compliance

3. ALTERNATIVE OPTIONS CONSIDERED & NOT RECOMMENDED

3.1 N/A

4. COMMENTS OF OVERVIEW & SCRUTINY

4.1 N/A

5. POST-DECISION IMPLEMENTATION

5.1 N/A

6. IMPLICATIONS OF THE DECISION

6.1 Council Key Priorities and Performance

6.2 Financial Implications

N/A

6.3 Policy Implications

N/A

6.4 Legal & Constitutional Implications

6.4.1 N/A

6.5 Community Impact

6.5.1 N/A

6.6 Environment & Climate Change Implications

6.6.1 N/A

6.7 Equality & Diversity Implications

6.7.1 N/A

6.8 Implications on Resources

6.8.1 N/A

6.9 Health & Wellbeing Implications

6.9.1 N/A

6.10 Local Government Reorganisation (LGR) Implications

6.10.1 N/A

7. RISK MANAGEMENT

7.1 N/A

8. BACKGROUND PAPERS– LOCAL GOVERNMENT (ACCESS TO INFORMATION) ACT 1985

8.1 N/A