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 – 9 July 2024
Executive Portfolio:	Executive Councillor for Corporate Services
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 headed up 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 2023 to March 2024.

The number of requests received by the Council in 2023-24 was 483; an increase on the previous year's total of 642 (a 33% increase).

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 2023-24; hereby, 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 arrangements 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 (IG) Team leads 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.

3.2 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 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, to replace Huntingdonshire District Council's Information Governance Group. The Board is made up of representatives of HDC, SCDC and Cambridge City Councils to ensure that the three councils work together to manage the data that the three councils hold 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.

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

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

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 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

5. INFORMATION SECURITY COMPLIANCE

5.1 Cybersecurity 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 3C ICT are still working with the Department for Levelling Up, Housing and Communities (DLUHC) 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.

5.3 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 DLUHC recommendations of the need for these systems.

5.4 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.

5.5 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.

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.

6.4 Individual requests made during the year were as follows:

	Received	Compliance with time frame
Data Rights Requests (including Erasure Requests, etc.)	26	14
SAR Reviews	3	3
ICO SAR Complaints	1	1

Table 1: Personal information rights requests 2023-24

6.5 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.

6.6 Requesters also have a right to complaint to the ICO in their capacity as the regulator. The Council received one complaint from the regulator this

year. Following the ICO's review of the case they upheld the Council's position, and no further actions were required.

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 IG team when an incident is logged 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 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

Table 2: Personal data incidents 2020-2024

7.4 20 incidents were reported in 2023-24, a decrease in the number of incidents from previous years. A breakdown of these is as follows:

Type of Incident (Category)	Number
Corruption or inability to recover data	1
Personal details inappropriately disclosed (e.g. via email or post)	13
Lost in transit	1
Unauthorised access or disclosure	1
Uploaded to website in error	1
Other	3

Table 3: Categories of personal data incidents 2022-23

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 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.

7.7 Updated guidance on sending information and how to share securely has been provided due to the volume of incidents relating to this type of incident, and where this occurs more than once across a service additional training and support is provided to identify and eliminate root causes of these incidents.

7.8 In January 2024 the process for reporting Data Protection incidents was changed to bring it into line with the reporting of ICT incidents and helpdesk calls. This enables better oversight and reporting against performance targets and provides a single point of reporting for all staff.

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 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.

8.4 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.

8.5 In 2023-24 (Apr – Mar) the council received a total of 642 requests under FOIA and EIR.

8.6 This represents a 33% increase in the number of requests received in the previous year. This is close to the number of requests received in 2019 and sees a return to pre-pandemic levels of requests to the Council.

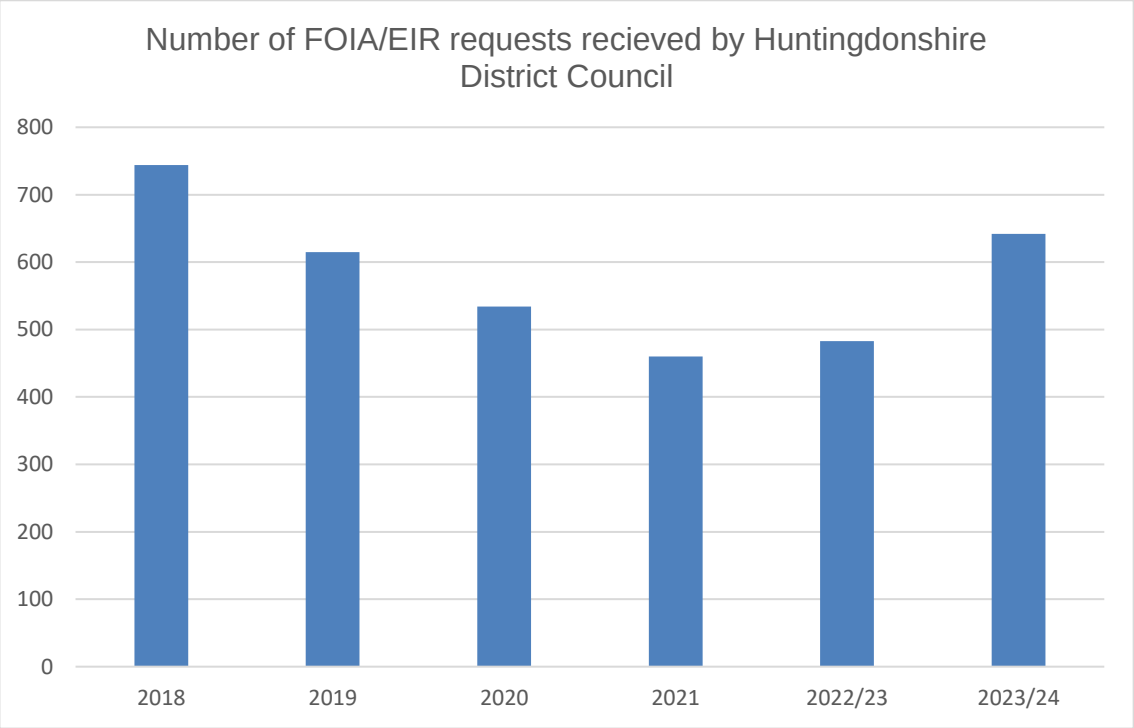

Chart 1: Information requests to HDC 2017-2023

8.7 The Council works to a target of 90% response compliance within 20 days as advised by the Information Commissioner. We achieved 81% in 2023-24 which is a slight decrease over 83% of the previous year.

8.8 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.

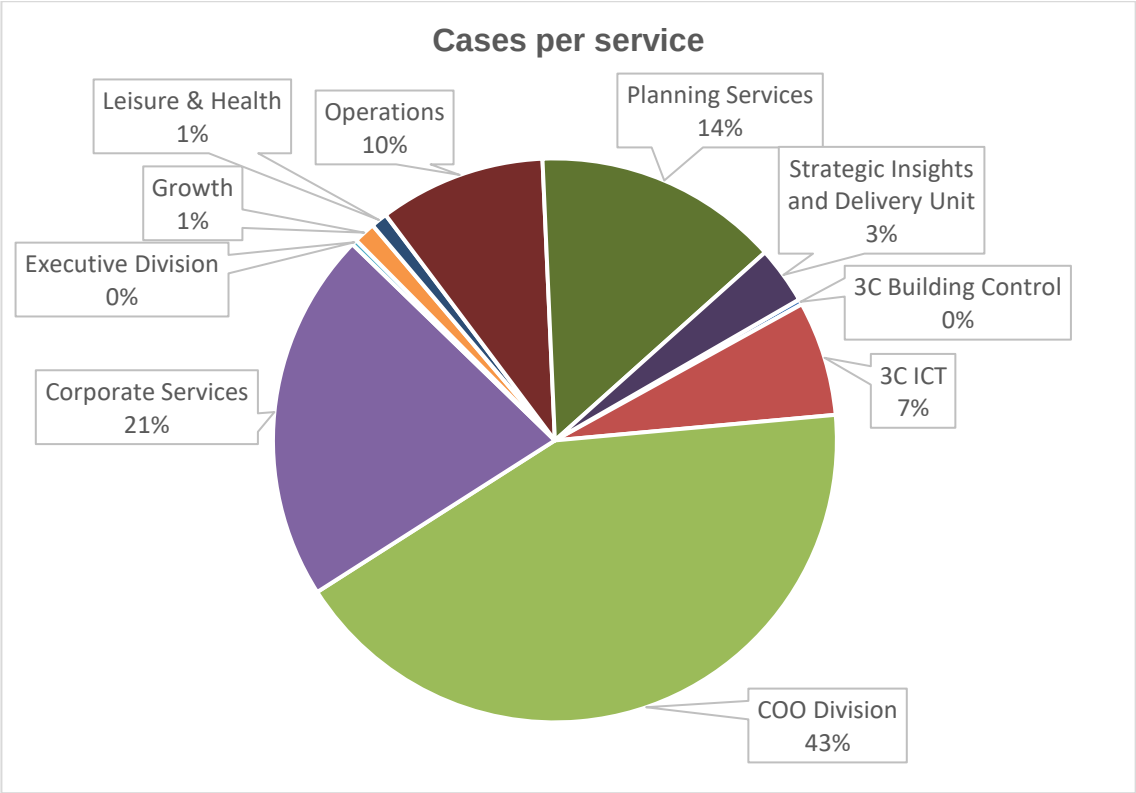

Chart 2: Number of requests per service area

8.9 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 the information was provided for most requests, with information being exempted in only 10% of cases. See breakdown of outcomes below.

Request Outcome	Count
All information provided	385
Some information provided; remainder exempt	15
Some information provided; remainder not held	14
Some information provided; remainder refused on cost	5
Exemptions applied to all information	50
Not held	98
Concluded outside of legislation	1
Withdrawn	33
Vexatious	0

Table 4: Outcomes to information requests 2023-24

8.10 The IG 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.

8.11 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	12	12
ICO Complaints	5	5

Table 5: Information request reviews and complaints to regulator 2023-24

8.12 None of the complaints investigated by the regulator resulted in any further review of the Council's decision.

9. LOOKING FORWARD

9.1 Ensuring ongoing compliance with Data Protection Legislation (DPA 2018 and UK GDPR) has been the focus of the Information Governance team.

9.2 An improved learning offering including quick reference guides and regular training for FOI Co-ordinators

9.3 In line with the Information Governance Action Plan there are updates planned for the DPIA process, as well as work to review and update the current suite of policies and Information Asset Registers within the organisation.

9.4 The Information Governance team will continue to work with Service areas to address gaps identified as part of the original gap analysis and subsequent health check report (on Data Protection Compliance) and provide updates during the Information Governance Group meetings.

CONTACT OFFICER

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