Pubic
Key Decision – No

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 – 27 September 2023
Executive Portfolio:	Councillor M Hassall – Executive Councillor for Corporate and Shared Services
Report by:	Information Governance Manager & Data Protection Officer
Ward(s) affected:	All Wards

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 2022 to March 2023.

The number of requests received by the Council in 2022-23 was 483; an increase on the previous year's total of 460 (a 5% increase).

Recommendation:

The Committee is

RECOMMENDED

    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 2022-23; 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.

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. Following the stepping down of the DPO/IG Manager in December 2022 a new DPO/IG manager joined the team in March 2023.

- 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.

- There is currently one vacancy for an Information Management Officer in the team, and recruitment is underway for this post.

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

3.4 This year has seen the retiring of the Information Governance Group (IGC) for Huntingdonshire District Council and the creation of a Joint Information Governance and Security Board. The Board is made up of representatives of Huntingdon District Council, South Cambridgeshire District Council and Cambridge City Council 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 July 2023.

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 2022-23 include:

- Management for inactive Teams sites;

- Guidelines for the corporate use of Instant Messaging services such as WhatsApp;

- Policy on Internal Reviews for FOIA, EIR and Data subject rights requests.

4.6 Lunch and Learn training sessions for Data Protection ran throughout the year - eight sessions were run between September 2022 and April 2023. These sessions were open to all staff in all Councils and were well attended.

5. INFORMATION SECURITY COMPLIANCE

5.1 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.

5.2 Recruitment of a dedicated Information & Cyber Security Lead Officer, the Council has increased its investment in cyber security, enabling 3C ICT to maintain its improved defence against ever changing threats.

5.3 The remaining areas in amber can now be found in green due to improvements made over the past year. Benefits from implementation and fine tuning of a central logging system have already been seen with the result of an improved process for using privileged network accounts.

5.4 3C ICT continue to work with the Department for Levelling Up, Housing and Communities (DLUHC) to reduce cyber risk. As well as completing the work on the central logging system, implementation of an internal vulnerability identification solution is underway which will allow 3C ICT to be more proactive in identifying and prioritising new vulnerabilities on all networked devices as they are released.

5.5 In quarter year 3 budget year 2023/2024, 3C ICT will start working with service areas running through the NCSC Exercise in a Box. This is an online tool which allows service areas to test how resilient they are to a cyber-attack in a safe environment.

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 requests made during the year were as follows:

	Received	Compliance with time frame
Data Rights Requests (including Erasure Requests, etc.)	21	12
SAR Reviews	2	2
ICO SAR Complaints	1	1

Table 1: Personal information rights requests 2022-23

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.

6.5   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.

6.6   There is a final right of appeal against a Decision Notice made by the Information Commissioner. These appeals are heard by the First Tier Tribunal (General Regulatory Chamber) Information Rights.

6.7   Following from a request received in May 2020, an internal review, and Decision Notice issued in 2021 the ICO's decision was appealed by requester. In November 2022 the Information Tribunal Council was passed its decision that Huntingdonshire Council should provide a fresh response to the original request of May 2020 as some information was not provided at the time of the response. This information was provided in line with the Tribunal Judgement.

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 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.

Figures indicate a decrease in reporting for the pandemic, with the expected root of this decrease to be both a change in working practice would mean staff are less clear on identifying where errors in practice were and decreased processing during the pandemic resulting in fewer incidents raised, as evidenced by one IG incident reported within April-July 2020 and four within the first eight months of that financial year.

	Incidents/breaches	Reported to ICO
2020-21	11	0
2021-22	25	2
2022-23	27	0

Table 2: Personal data incidents 2020-2023

7.4 27 incidents were reported in 2022-23. None of these were assessed to meet the threshold for reporting to the ICO. A breakdown of these is as follows:

Type of Incident (Category)	Number
Personal details inappropriately disclosed (e.g. via email or post)	17
Lost or stolen paperwork	1
Non-secure disposal of hardware (eg mobile phones/laptops)	1
Non-secure disposal of paperwork	1
Uploaded to website in error	3
Technical security failing	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 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.

7.7 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.

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 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 timeframe of twenty 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 2022-23 (Apr – Mar) the council received a total of 483 requests under FOIA and EIR.

8.5 This represents a 5% increase in the number of requests received in the previous year. The longer-term trend in FOIA/EIR request numbers received by the Council is that of a decline from the high point of nearly 750 received in 2018.
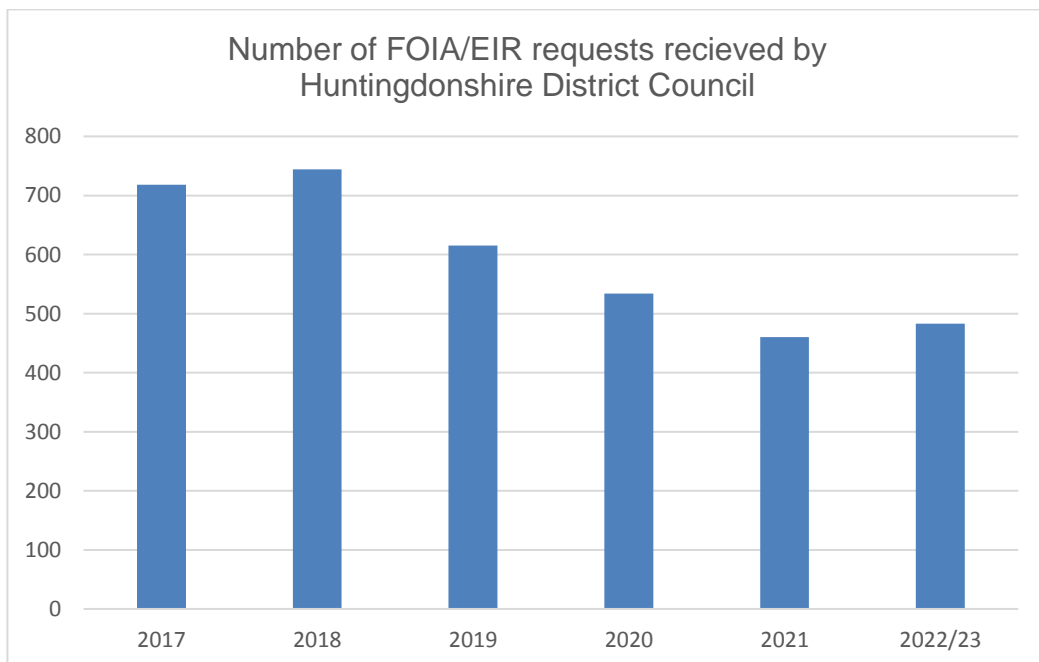

Chart 1: Information requests to HDC 2017-2023

8.6 The Council works to a target of 90% response compliance within 20 days as advised by the Information Commissioner. We achieved 83% in 2022-23 which is an improvement on the 81% of the previous year.

8.7 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.
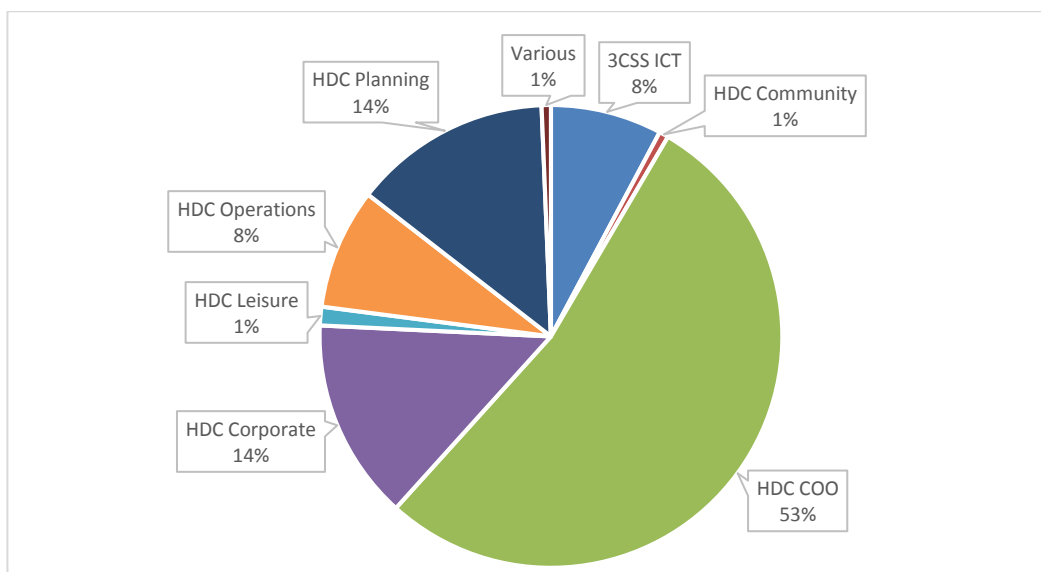

Chart 2: Number of requests per service area

8.8 Access to information acts such as FOIA and EIR provide a limited right of access. Some information may be withheld if an exemption applies to its disclosure. All the information was provided for most requests. See breakdown of outcomes below:

Request Outcome	Count
All information provided	348
Some information provided; remainder exempt	12
Some information provided; remainder not held	13
Some information provided; remainder refused on cost	1
Exemptions applied to all information	44
Not held	97
Concluded outside of legislation	2
Withdrawn	28
Vexatious	1

Table 4: Outcomes to information requests 2022-23

8.9 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.

8.10 Requestors have the right to an 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	16	15
ICO Complaints	6	5

Table 5: Information request reviews and complaints to regulator 2022-23

8.11 Of the six complaints investigated by the regulator, one case was withdrawn, two were concluded informally by the ICO, and two resulted in Decision Notices. The Decision Notices upheld the Council's findings, and resulted in no further action to date. One investigation is still with the regulator and awaiting an outcome. All Decision Notices are published on the [ICO's website](#).

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 lunch and learn, quick reference guides and regular training for FOI Co-ordinators.

9.3 An updated Information Requests system is scheduled for October 2023 within which the team are aiming to increase the availability of reporting for services and senior stakeholders.

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

9.5 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