HUNTINGDONSHIRE DISTRICT COUNCIL

Title/Subject Matter:	Annual report on HDC compliance with the Freedom of Information (FOIA) & Environmental Information Regulations (EIR) Acts
Meeting/Date:	January 2021
Executive Portfolio:	Executive Councilor for Digital and Customer
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 lead on Information Requests, Data Protection Compliance, Data Privacy and provide additional advice around Information Management. The team is headed up by the Information Governance Manager who is also the Data Protection Officer.

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 with regard to protecting personal data and covers the period Jan 2020 to Dec 2020.

The number of requests received by the Council in 2020 (534) decreased from the previous year, (615).

Recommendation(s):

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

1. PURPOSE

1.1 The purpose of this report is to provide an update on Information Governance activity and performance during 2020 (January – December); hereby, highlight any issues encountered and actions to be undertaken to improve performance.

2. SCOPE

2.1 It provides:

- An overview of the current arrangements in place to monitor the Information Governance at the Council.

- An update on performance relating to:
  - Freedom of Information (FOI) Act / Environmental Information Regulations (EIR) Requests
  - Data Subject Access Requests
  - Personal Data Breaches

3. BACKGROUND

3.1 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 in order to minimise risk to the public and staff and to protect its finances and assets.

3.2 Information Governance describes the holistic approach to managing information by implementing processes, roles and metrics to transform information into business assets. This includes coverage around access to information, data quality, information management, information security and information sharing, data privacy and Data Protection compliance.

4. ORGANISATIONAL ARRANGEMENTS

4.1 The Information Governance Service for Huntingdonshire District Council (HDC) is currently provided by 3C ICT Shared Service. This also serves South Cambs District Council and Cambridge City Council. The Information Governance (IG) Team lead on Information Requests, Data Protection Compliance, Data Privacy and provide additional advice around Information Management; whilst the 3C ICT provide support on Information Security.

4.2 The IG Team consists of six members, four of whom, including the current

Data Protection Officer (DPO), joined in 2020. The DPO is responsible for leading the IG team. As this is a shared service, the DPO is also the DPO for all three Authorities.

4.3 Updates on IG arrangements across Huntingdonshire District Council (HDC) are provided to the Information Governance Group (IGG). This Group is designed to facilitate the necessary engagement to ensure the relevant accountability of staff across the various services and to assist in driving any improvements required. It is chaired by the Senior Information Risk Owner and comprises of number of managers / heads of services across most service areas within the Council.

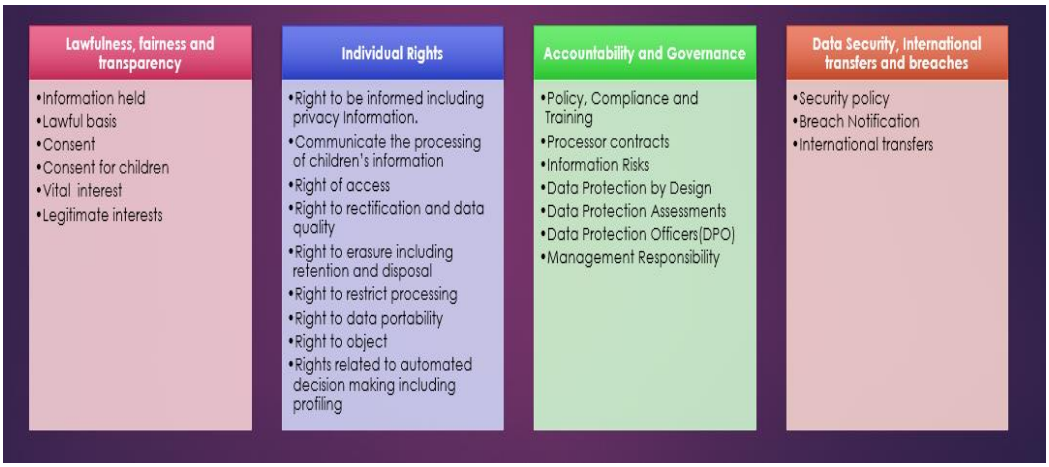
4.4 The Information Governance Group meets quarterly and last met early November 2020.

5. DATA PROTECTION COMPLIANCE

5.1 The IG team carried out a review of the Data Protection arrangements this year to determine the areas for priority action.

5.2 The main areas covered included: Lawfulness, Fairness and Transparency, Individual Rights, Accountability and Governance, Data Security, International Transfer and Breaches. Each area consisted of a number of sub-categories.

The scope for each category is provided below:



The overall finding from the review was that, whilst appropriate procedures were generally in place, these were generally informal, incomplete, and/or inconsistently applied.

5.3 Improvements were required in the following areas:

Area	High Level Finding	Risk	Actions needed
Information Asset Registers / Flows	Although some Information Asset records were held by Service areas; we do not hold a central repository. These should be reviewed regularly to ensure information is accurate and held centrally.	The risk here is that there is no overview of our processes / systems which could result in delays to information requests; inappropriate controls being in place; no clear view on dependencies in terms of ICT systems when a change is made; etc.	Review of existing information to ensure this is up to date; and collate this centrally.
Records of Processing (Article 30)	Although the Information Asset Register does collect most of the information required for Article 30; this is not held centrally; in addition to this, more information would be required on disclosures and transfers.	There is a risk that information is inappropriately being transferred (i.e. there may not be appropriate adequacy arrangements or appropriate technical safeguards in place)	Review existing information to ensure transfers are documented.
Policies	Although there are some policies accessible on the Council's intranet pages, a number of these are out of date. To add to this, there are also additional IT Policies located within a repository (Protocol Policy) which is not accessible to all staff as they are not published on the Intranet.	The risk is that staff are not aware of their obligations and therefore put the Council resources at risk.	Policies need to be reviewed and published as appropriate.
Training Arrangements	The requirement by the ICO is that training is undertaken at least every two years. New starters are required to undertake e-	Although not in breach of the Act, by undertaking training every 2 years, this frequency is not in line with other partners in the public	Need to review Information Governance training provision including content; reporting and frequency for

Area	High Level Finding	Risk	Actions needed
	learning as part of their induction process. For many existing staff, e-learning was undertaken in preparation for GDPR in 2018. This therefore means a number of staff will be coming up to the 2-year threshold for retraining. To date, there has been limited communication to enforce the requirement for refresher training for existing staff.	sector (e.g. NHS). This therefore creates a hurdle when signing up to Information Sharing Agreements.	undertaking training. The requirement for refresher training will need to be reinforced.
Information Sharing Arrangements	Although there are Information Sharing Agreements in place across the Council, there is no central register for this. There is no clear visibility if there are appropriate contracts / sharing agreements in place.	If a contract is not in place where data is being processed on behalf of the Council by a Data Processor; this is likely to be a breach of GDPR.	An Information Sharing Log needs to be created. The Information Asset Register work (identified above) is also likely to identify where Contracts are needed.
Incorporation of Privacy by Design in Projects	Data Privacy Impact Assessment (DPIAs) are completed; but it is unclear if this is always the case. DPIAs are currently treated as standalone documents to be completed at project initiation. Not all changes, go through a standard project process.	DPIAs may not be completed and therefore privacy risks may either not be identified / identified in a timely manner.	The DPIA process and document to be reviewed and communicated. Its requirement needs to be better communicated and/or integrated with Project / Change processes.

5.4 The actions to address the above have been factored into the ongoing IG forward plan 2020/21.

5.5 Updates to monitor the status and progress on this will be provided to the Council's Information Governance Group (IGG).

6. PERFORMANCE UPDATE

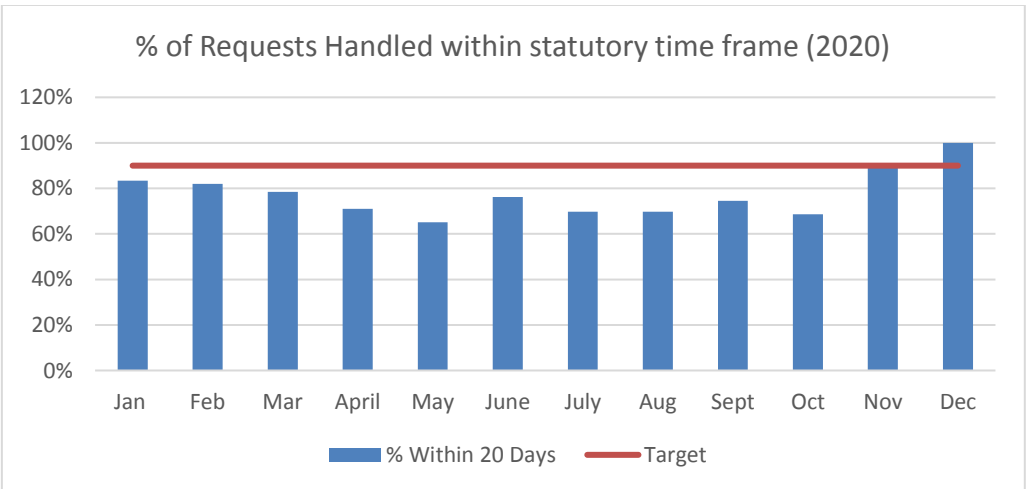
6.1 FREEDOM OF INFORMATION / ENVIRONMENTAL REQUESTS

The public has the right of access to information held by the Council under the Freedom of Information Act. The Freedom of Information Act (FOI) works alongside the Environmental Information Regulations (EIR).

6.2 Freedom of Information requests relate to requests for information that are not dealt with as part of the day-to-day business processes.

6.3 The 3C ICT Information Governance has implemented a shared request management system for handling information requests. Ownership of the response to these requests is placed on Services areas by means of key responders and champions being designated and responsible for ensuring their Service responds within the timeframe. An Information Governance Officer coordinates all formal requests and allocates specialist support from the Information Governance team where Officers require this.

6.4 The Council works to a target of 90% response compliance within 20 days (statutory requirement) as advised by the Information Commissioner. We achieved 77%. Breakdown for each month in 2020 is provided below.



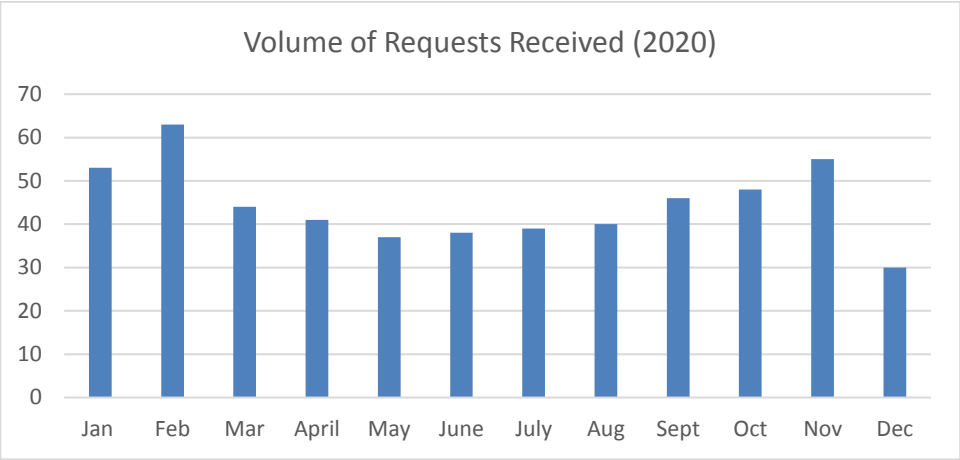
6.5 Reasons for this included resource shortages within the Information

Governance Team within the first half of the year and Service Areas not being able to respond to requests for data on time due to priorities being diverted as a result of COVID-19.

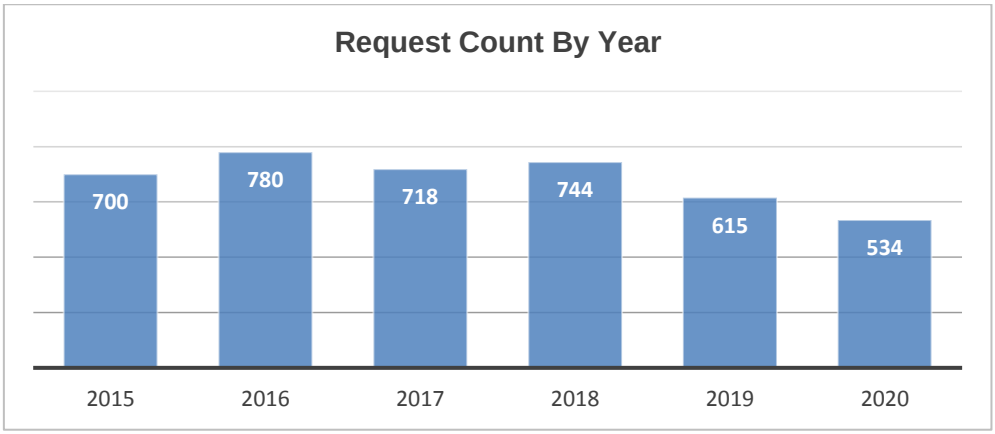
6.6 An Information Officer has since been recruited in June 2020.

6.7 The importance of responding to these on time and correctly is also being reinforced through the Information Governance Group Meetings.

6.8 For 2020 (Jan – Dec) the council received a total of 534 requests under FOI and EIR.

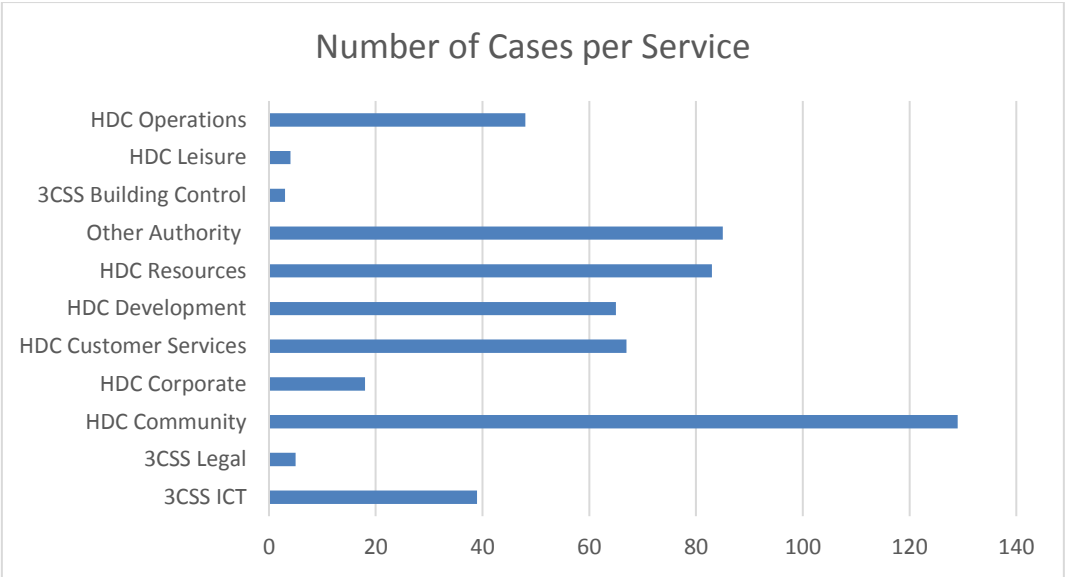


6.9 This represents a 13.1% decrease in the number of requests received in 2019. The graph below demonstrates the year on year trend in the number of FOI requests received since 2015.

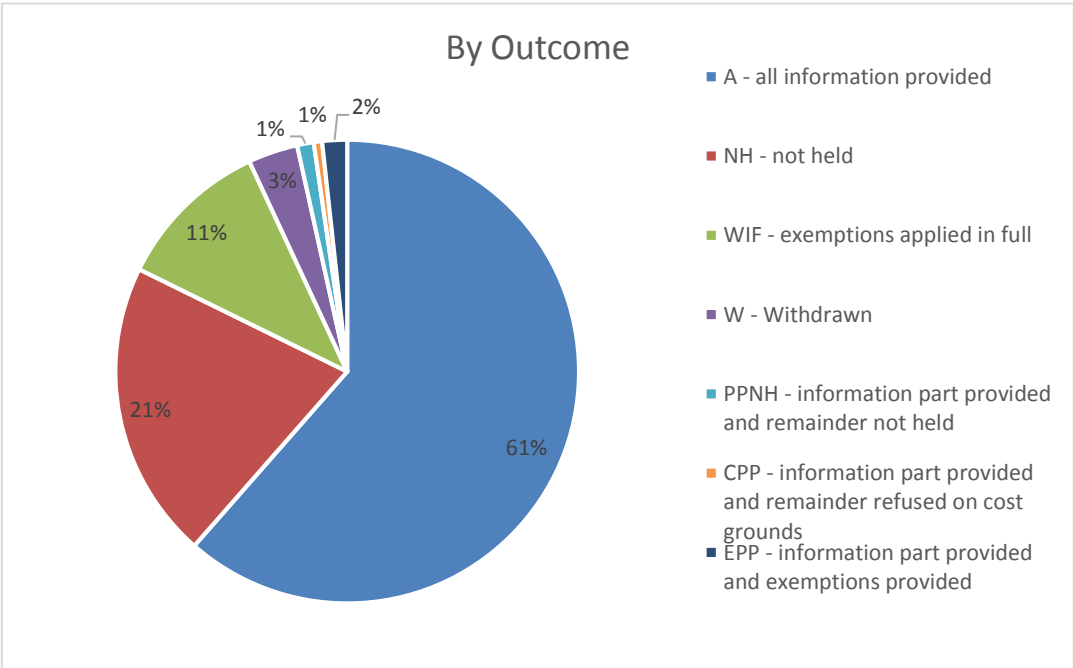


6.10 Community Services have received the most cases and reasons may vary depending on what is happening during period of interest.

There were also a number of requests that were relating to services that other Authorities provided.



6.11 All the information was provided for the majority of requests. See breakdown of outcomes below.



6.12 A great proportion of the information of regular interest is now proactively

published and updated on a monthly basis. The IG team will continue efforts to support Services to increase this transparency offering via an Open Data Strategy.

6.13 The IG team have also recently developed reports, which are shared with the Information Governance Group on a quarterly basis, to understand trends, and to help departments focus on what should be uploaded onto their publication scheme.

6.14 Requestors have the right to an 'internal 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
Internal Reviews / Complaints	9
ICO Investigations	4

Whilst these have been investigated by the regulator (ICO) these have resulted in no further action.

7. INDIVIDUAL DATA REQUESTS

7.1 The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulations (GDPR). Data protection is primarily concerned with personal data about individuals rather than general information.

7.2 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.

7.3 Individual requests made during the year were as follows:

Other Requests	Received	Compliance with time frame
Subject Access Requests (SAR) (including Erasure Requests, etc.)	16	5 (2 still open as of 6/1/2021)
SAR Complaints	0	-

7.4 Reasons for delays included:

- lack of Information Management resource being in place for the first half of the year
- lack of awareness by officers to put requests on hold whilst awaiting identification or clarification;
- resources being divert due to COVID.

A new Information Officer was recruited within the IG team in June this year.

The importance of prompt response and the need for training of all staff is also being reiterated through IGG, as well as additional training for Information Champions being given as appropriate.

8. PERSONAL DATA BREACHES

8.1 The guidance on notification of data breaches under the Data Protection Act / GDPR is that where a breach incident is likely to result in risk to the rights and freedoms of individuals, the Council must inform the ICO within 72 hours and 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.

8.2 As result, the IG 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.

This is performed by the IG team when an incident is logged by a Service Area.

8.3 The IG Team have also developed a register to log incidents / near misses relating to personal data. This allows trends to be identified, with the view to establish if any specific training needs are required or if any actions are needed to enhance the current measures to prevent the likely reoccurrence.

8.4 **Performance Data – Data Breaches**

Although 11 incidents were reported in 2020 (Jan – Dec). None of these met the threshold for reporting to the ICO. A breakdown of these is as follows:

Type of Incident (Category)	Number	Reported to ICO
Personal details inappropriately disclosed (e.g. via email/ shared/published on website)	9	Not reportable to ICO
Lost or stolen hardware	1	Not reportable to ICO
Technical Security failing	1	Not reportable to ICO
Total	11	

8.5 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.

8.6 A quarterly update on incidents is now provided to the IGG to ensure visibility and ensure any improvements needed are discussed and followed through as appropriate.

9. TRAINING

9.1 To ensure organisational compliance with the law and relevant guidance relating to Information Governance (IG), staff must receive appropriate training.

9.2 In 2018, when the GDPR legislation was implemented, staff underwent compulsory training via the e-learning module.

9.3 In addition to this, all new starters who manage confidential information are expected to undertake training on handling confidential information.

9.4 In 2021, the HR team are looking to implement a new Learning Management System. The understanding is that this should facilitate easier reporting. The IG Team intend to provide updates on training uptake to the IGG once this done.

10. LOOKING FORWARD

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

10.2 The Information Governance team will continue to work with Service areas to address gaps identified as part of the Gap Analysis undertaken (on Data

Protection Compliance) and provide updates during the Information Governance Group meetings.

11. KEY IMPACTS/RISKS

11.1 The key impact of non-compliance with FOIA/EIR and the Data Protection Act along with GDPR is public scrutiny from the regulator.

11.2 Poor service or inadequate information management will lead to loss of trust from our customers. Inability to act in accordance with the Act and the Governments accountability and transparency directive will lead to reputational damage.

11.3 Furthermore, the right of access is bound with the Human Rights Act in respect of the right to privacy. Unlawful disclosure of personal information may lead to publicly enforced audit, warning, reprimand, corrective order and fine by the regulator.

12. WHAT ACTIONS WILL BE TAKEN

12.1 Compliance will Data Protection Legislation will continue to be monitored. Actions as identified in Section 5.3 will be undertaken. Updates will be provided via the Information Governance Group.

13. LINK TO THE LEADERSHIP DIRECTION

13.1 Supports the objective to become a customer focused organisation under the strategic priority of becoming a more efficient and effective Council.

14. CONSULTATION

14.1 None

15. LEGAL IMPLICATIONS

15.1 HDC must comply with the law concerning FOIA/EIR and Data Protection Act

16. RESOURCE IMPLICATIONS

16.1 There are no direct resource implications arising from this report.

17. OTHER IMPLICATIONS

17.1 None

18. REASONS FOR THE RECOMMENDED DECISIONS

18.1 This paper updates Members on how requests under FOIA/EIR have been dealt with by HDC.

18.2 This report is for information purposes only, unless otherwise.

19. LIST OF APPENDICES INCLUDED

19.1 None

20. BACKGROUND PAPERS

20.1 None

CONTACT OFFICER

Madelaine Govier
Information Governance Manager & Data Protection Officer (3C ICT)
Infogov@3csharedservices.org