HUNTINGDONSHIRE DISTRICT COUNCIL

Title/Subject Matter:	Annual report on HDC compliance with the Freedom of Information (FOIA) & Environmental Information Regulations (EIR) Acts
Meeting/Date:	23rd January 2019
Executive Portfolio:	Executive Councillor for Digital and Customer
Report by:	Information Governance Manager & Data Protection Officer
Ward(s) affected	All Ward(s)

EXECUTIVE SUMMARY:

The Information Governance (IG) service falls under the 3C ICT shared service with Huntingdonshire District Council and South Cambridgeshire District Council. The IG service produces and implements the Information Governance framework regarding Access to information, Information Management and Data Protection and information security, in accordance with legislation. The small team is headed up by the Information Governance Manager who is also the Data Protection Officer; this is a new independent statutory (whistleblowing role) mandatory for local authority.

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 for the first time the Councils performance with regard to protecting personal data and covers the period Dec 2017 to Dec 2018.

The number of requests received by the Council in 2018 (789) increased from the previous year,(718) following a long period of growth.

A shared request management system was integrated in July 2017. This new process places more ownership on the Services whereby key responders and champions are designated and responsible for ensuring their Service responds within the timeframe. The Information Governance Officer coordinates all formal requests and allocates specialist support from the

Information Governance team where officers require this. We are about to initiate an upgrade, improving the functionality to make it easier for teams to self-serve and rewriting all of the request templates and guidance documents. Disclosure log publication of FOI requests will begin in February.

This new process has been successful. After a sustained period functioning below target pre 2016, the Council now consistently achieves above 90% and even 100% compliance. See appendix A.

There was a noticeable dropping off in October and November; this was a direct result of staff resource issues. December saw a return to upward incline

Recommendation(s):

Corporate Governance Committee is asked to comment on this report.

1. PURPOSE

1.1 The purpose of this report is to:

- Report on the requests for information received by the Council under FOIA & EIR and highlight any issues encountered and actions to be taken to improve performance.

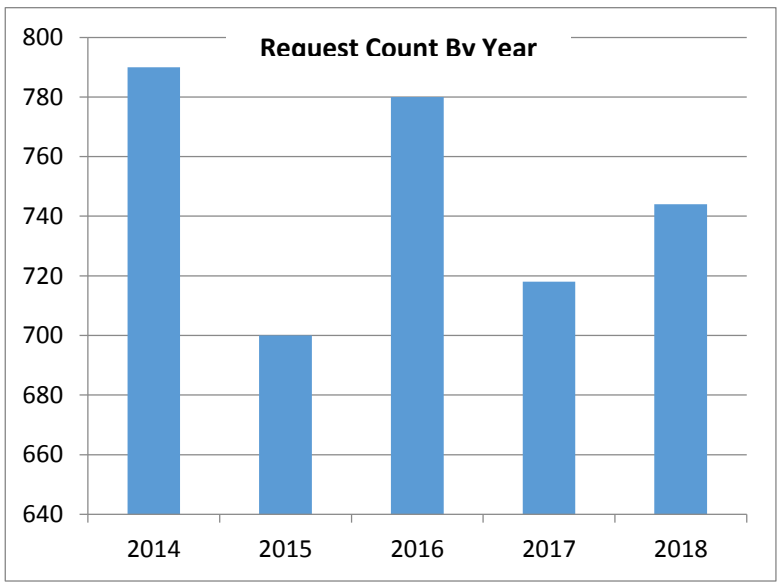
2. BACKGROUND

2.1 The public has the right of access to information held by the Council under the Freedom of Information Act. The Freedom of Information Act (FOI) works alongside the Environmental Information Regulations (EIR). Service areas are responsible for responding to requests, and 3C ICT Information Governance Team manage the process, provide support and ensure compliance. The Council works to a target of 90% response compliance within 20 days (statutory requirement) as advised by the Information Commissioner.

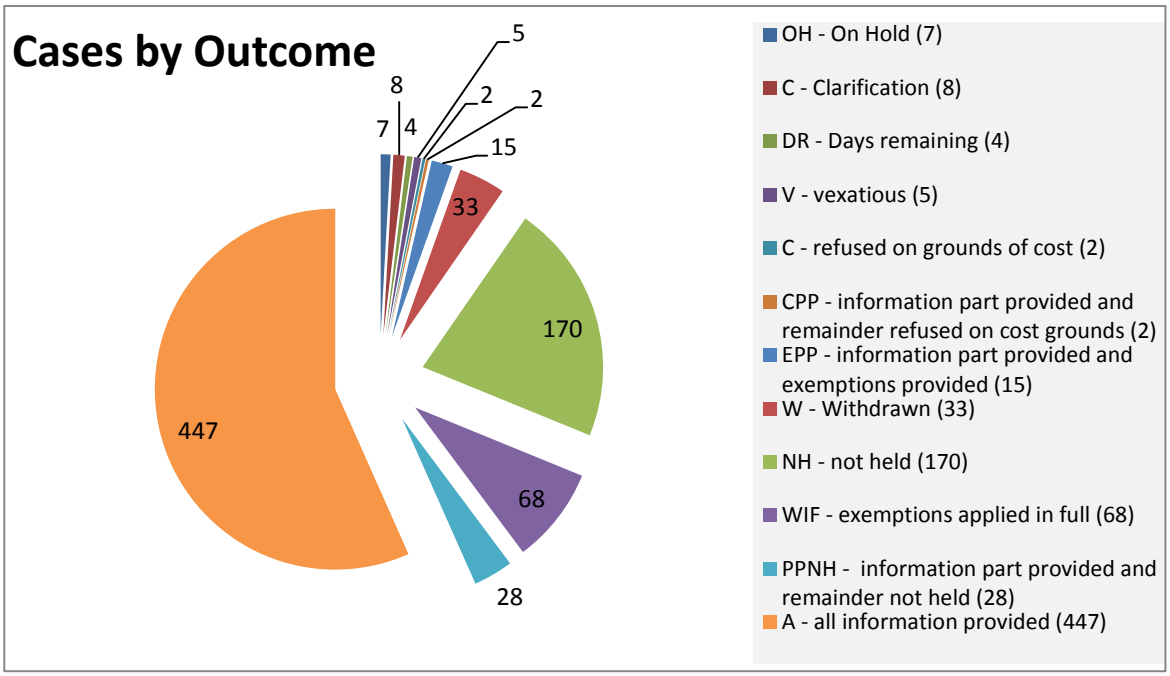
2.2 The Council receives many requests for information in all service areas. Most are dealt with as part of the day-to-day business, but where a request is out of the ordinary, specifically invokes the legislation, or is likely to engage an exemption, it is formally logged and processed. This report relates to those formally processed requests.

3. REQUESTS FOR INFORMATION

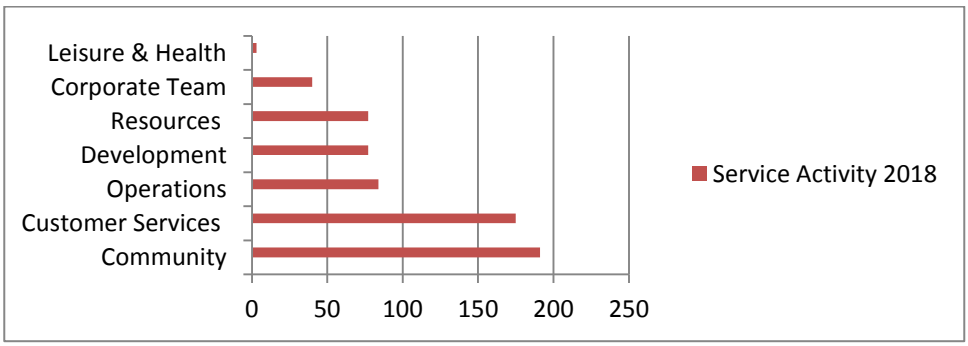
3.1 Total requests received in the report period is 789.



3.2 The majority of requests are concluded by all of the information provided. A greater 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, planned for implementation this year whereby we will work with our partners at Cambridgeshire County Council and to standardise and regularly publish comparable data from the three partners including data required to be published under the Transparency Code directive, providing a valuable district data set.



3.3 Customer Services and Community receive the highest demand. Business rates information is now proactively published so that although logged they are handled within minutes by pointing the requester to the website, reducing the burden on the Revenues and Benefits Service. Information relating to the environment is consistently in demand we are working with the team to identify whether data sets can be proactively published.



Community Custo

3.4 The source of requests is becoming more difficult to assess, since many are sent from anonymous webmail addresses, therefore this is not reported.

3.5 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. During the report period 9 internal reviews were undertaken (reduction from the last report),

4 DATA PROTECTION

The Council collects and holds a wide range of personal information about our tenants, residents and the users of our services. This information helps us to provide services and assist our customers.

4.1 The Data Protection Act (DPA) provides a framework to ensure that personal information is handled appropriately, fairly and securely. Note the legislation went through an overhaul in May 2018 when the General Data Protection Legislation (GDPR) came into force and was enacted in to UK law by the Data Protection Act 2018. The Council must process personal data in accordance with the Data Protection Principles, as follows:

4.2 Information must be processed fairly and lawfully. This means that the individual providing personal information to Council services must clearly understand why their data is needed, who it will be shared with, giving them a clear indication of how their personal data will be used.

4.3 Personal information is collected for specified, explicit and legitimate purposes, and ensuring that the information collected is not processed in a manner incompatible with those purposes.

4.4 Using personal information only for the purposes specified by the authority to the Information Commissioner Office (ICO)

4.5 Processing is adequate, relevant and limited to what is necessary.

4.6 Ensuring that personal information collected is accurate, kept up to date, and inaccurate, information is erased or rectified without delay.

4.7 kept in a form which permits identification of data subjects for no longer than is necessary.

4.8 Ensuring that personal data is kept securely. The Council is required to take appropriate technical and other measures to prevent unauthorised or unlawful

access to personal information, or accidental loss, destruction or damage of personal information.

4.9 Ensuring that personal information about individuals is not shared with other people or organisations, except in the circumstances described by the Act. These exceptions to the Act include when information could assist in the prevention and detection of a crime, the apprehension or prosecution of offenders and matters of taxation and where disclosure is required by law or in connection with legal proceedings.

4.10 Providing individuals with access to information held by the Council about them, through responding to Subject Access Requests and by upholding their enhanced rights. The Council must now be much clearer about what we do with individual's personal data through our Privacy Notices. Other rights include the right to rectification, erasure, to restrict processing, data portability, and to object to processing.

4.11 The Council is now required to prove accountability - it does this by recording its processing activity (The Council maintains an Information Asset Register) and is required to have processing agreements or sharing agreements in place with all third party processors of personal data.

4.12 If the Council is in breach of the above data protection principles, it can have a significant impact on the individual(s) affected. In particular, the loss or unauthorised sharing of personal information can have serious impacts, ranging from harassment to identity theft. In such circumstances, public bodies such as the City Council can be liable for significant fines.

4.13 The Information Commissioners Office (ICO) receives reports of breaches of the Data Protection Act and makes decisions in each case. The ICO under the new law has the power to impose fines of up to £17million (previously the maximum was £500,000) for breaches of data protection obligations, as well as issuing enforcement notices and requiring organisations to sign undertakings to improve their practices.

5.0 BREACHES OF PERSONAL DATA

5.1 Their guidance on notification of data breaches under the new law 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 hrs and if its 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. The Council has a new incident policy to reflect this.

5.2 The Council considers the following factors as laid out in the (ICO) guidance when considering what should be reported.

Potential detriment and adverse affect to the data subject is the overriding consideration. This includes emotional distress, and includes information about the private aspects of a person's life becoming known to others. The extent of detriment depends on the volume of the data and its sensitivity. Where there is little risk that individuals would suffer significant detriment there is no need to report.

5.3 The Councils Performance - Breaches of Personal Data

The Council maintains a register of incidents relating to incidents or near misses regarding personal data so that we can identify risks and act to mitigate the likelihood of reoccurrence and continually improve In 2018 the following incidents were recorded.

Document sent in error to wrong recipient	4	1 reported to ICO. No notice of Investigation has been received.
Email sent to wrong recipient or unnecessary disclosure of others personal email address	2	Not reportable to ICO
ICT Hardware Stolen	1	Not reportable to ICO
Personal data unnecessarily published on the web site	2	Not reportable to ICO
Personal data wrongly disclosed	1	Reported to ICO – No notice of investigation has been received

6.0 Rights Request Handling & Complaints

6.1 The Information Governance Team also coordinate request relating to individuals rights such as right to request access to the personal data the Council hold), 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 .

Personal Data of third parties	13
Subject Access Request	13
Rights request	3

6.2 Complaints Received

Internal Review FOI	7
Subject Access Request Complaint	7
Official Complaint made via the ICO Includes FOI & SAR	7

Whilst these have been investigated by the regulator (ICO) these have resulted in no action or they have found in the Councils favour.

7.0 ORGANISATIONAL DATA PROTECTION MEASURES

7.1 Increased awareness of data protection further to this year's work across the authority in preparation for the changes to legislation (GDPR), has resulted in more enquiries especially around information sharing and safe disposal of information and retention practices. This is a positive outcome for the council, as staff are more aware of data protection and vigilant to areas of risk.

7.2 An Information Governance Board meets quarterly to review issues and drive improvements in the Council's approach to information security matters. Membership includes managers representing services that handle a high volume of personal data, The Group Is chaired by the Senior Information Risk Owner

7.3 An Information Governance Accountability Framework has been proposed by the Data protection officer as a means to imbed data protection ethos across all levels of the Council. It reinforces the requirement to embed a robust accountability structure (see appendix B) and regular engagement with those parties is scheduled. This involves the nomination of Information Asset Owners. The Data Protection Officer and Senior Information Risk Owner meet on a monthly basis.

7.4 The IG team have prepared a policy portal which contains up to date data security suite of policies, these alongside other IG framework policies will be accessible in a one stop shop on the Information Governance 3C intranet. Numerous Information governance policy and guidance have been updated or created to reflect the enhanced accountability measures under the new Data Protection Legislation.

7.5 Staff training and awareness of data protection continues to be key to data protection compliance. We have prepared a Data protection essentials policy All staff including new entrants will be required to demonstrate they have read and understood this.

7.6 In addition to new staff, all existing staff with access to Council IT accounts are required to complete the Cyber Security and Data Protection e-learning module by Feb 2018.The team are monitoring to ensure this is achieved. FOI e-learning training will also be rolled out in the next few months

7.7 GDPR awareness training seminars were run for staff and Members. Specific training requirements are identified in the Training Needs Assessment and rolled out in an annual programme.

8.0 LOOKING FORWARD

8.01 The implementation of the GDPR into UK law of has been the focus of the Information Governance team. Preparation for the Council to comply with the tighter legislation has included many work streams and focused on the following key legislative changes

8.02 Service level reports with 10 actions were produced as a method to record tasks and monitor the progress to make the necessary compliance changes, to enable scheduled conclusion of tasks. A GDPR consultant has assisted with this work The Council is in a satisfactory position in terms of compliance. The IG team have produced a 2018/19 forward plan which underwent review by SMT and the Information Governance Board The plan schedule's the final phase to instigate the compliance objectives and contains 53 tasks including the proposal of a number of projects to improve data quality and records management to better equip the council to manage data both in the short and long term.

9.0 KEY IMPACTS/RISKS

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

10 WHAT ACTIONS WILL BE TAKEN

10.1 The Information Governance Accountability Framework will be implemented:

10.2 Service specific FOI training on the exemptions. Clear guidance resource

and response templates produced including improved records management methods.

Compliance with GDPR will be monitored and work will continue.

10.3 An FOI disclosure log published via the Councils web site.

10.4 An Open Data strategy to manage the process; the quality and frequency of publication of the Councils key assets and compliance with the Transparency Code directive. To enable data to be given the widest publication but enabling correlation with partner data across the district.

11.0 LINK TO THE LEADERSHIP DIRECTION

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

12.0. CONSULTATION

12.1 None

13.0 LEGAL IMPLICATIONS

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

14.0 RESOURCE IMPLICATIONS

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

15.0 OTHER IMPLICATIONS

15.1 None

16.0 REASONS FOR THE RECOMMENDED DECISIONS

16.1 This paper updates Members on how requests under FOIA/EIR have been dealt with by HDC. The author suggested a broader scope to the report to in future include compliance with requests handled under the Data Protection Act/ The General Data Protection Regulations. These relate to requests for the personal data of individuals. As well as an overview of the Councils 'Open' data. Neither have previously been included in this annual report, but have been included here.

16.2 Members of the Corporate Governance Committee are asked to comment on the contents of this report.

17.0 LIST OF APPENDICES INCLUDED

17.1 Appendix A - Percentage of Requests Handled Within the Statutory Time frame

18.0 BACKGROUND PAPERS

18.1 None

CONTACT OFFICER

Jo Brooks
Information Governance Manager & Data Protection Officer (3C ICT)
01954 713318

Appendix A - Percentage of Requests Handled Within the Statutory Timeframe