

INFORMATION GOVERNANCE - ANNUAL REPORT 2015

SUMMARY

- 1.1 This report provides members with a summary report on the key activities carried out by the Information Governance Team in 2015.

RECOMMENDATIONS

- 2.1 To note the annual report.

REASON FOR RECOMMENDATIONS

- 3.1 The Audit and Accounts Committee is responsible for providing assurance to the Council on the effectiveness of the governance arrangements, risk management framework and internal control environment.

SUPPORTING INFORMATION

- 4.1 As part of the quarterly Governance Update report, Members have received updates on the work of the Information Governance team and statistics regarding the Freedom of Information (FOI) requests, Subject Access Requests (SARs) and any issues around compliance with the Data Protection Act. Previously members have received an annual Freedom of Information report. This year, to reflect the Council's investment in the Information Governance Team, the annual report has been expanded to reflect all aspects the team's work. The Head of Governance and Assurance's full report is attached at Appendix 2.

Freedom of Information :

- 4.2 The Council received 1,327 requests under the Freedom of Information Act during 2015. FOI requests totalled 1,124 and Environmental Information Regulation (EIR) requests totalled 203. Of the 1,327 requests, 1,000 (75%) were completed in full, with a further 68(5%) still in progress as at 31 December 2015. The Council refused 221 requests (16%) because it was able to either

- Apply an exemption under the Act;
- The Council did not hold the information; or
- The request would take longer than the “appropriate limit” (18 hours) to complete.

Note: The report in Appendix 2 provides more detail on the exemptions applied.

The number of requests withdrawn by the applicant in the year was 34 (3% of FOIs received.), while 4 requests were transferred to other local authorities.

- 4.3 The Council received 33 less requests in 2015 than it received in 2014. Table 1 below shows the number of FOI/EIR requests received since the Act came into force.

Table 1: Number of FOI/EIR Requests Received by Calendar Year

Year	Number of FOI/EIR Requests
Jan - Dec 05	183
Jan - Dec 06	239
Jan - Dec 07	250
Jan - Dec 08	358
Jan - Dec 09	581
Jan - Dec 10	685
Jan - Dec 11	913
Jan - Dec 12	923
Jan - Dec 13	1,209
Jan – Dec 14	1,360
Jan – Dec 15	1,327

- 4.4 The Act allows for an applicant to lodge an appeal against a refusal to provide information. In 2015 the Council received 3 appeals. These were all thoroughly investigated by the Appeals Officer and 1 appeal was successful in overturning the original decision to apply an exemption.

Data Protection – Subject Access Requests

- 4.5 A Subject Access Request is a written request from an individual to see information held on them.
- 4.6 The Council received 63 Subject Access Requests (SARs) in 2015. This was a 21.2% increase over the level received in 2014. Table 2 shows the number of SARs received each year since July 2009, when a formal recording system was introduced.

Table 2: Number of SARs Received by Calendar Year

Year	SARs Received in Year	SARs Completed in Year
July - Dec 09	31	15
Jan - Dec 10	28	30
Jan - Dec 11	40	45
Jan - Dec 12	38	52
Jan - Dec 13	36	28
Jan – Dec 14	52	55
Jan – Dec 15	63	63

- 4.7 All Subject Access Requests have to be completed within 40 calendar days, a great deal of flexibility is required to adhere to this deadline. We have implemented an SAR procedure to ensure that we receive the information promptly from the relevant departments. The volume of files required to satisfy each request fluctuates based on the Council's involvement with the data subject, the majority of requests relate to social care files which tend to be large files; an example include 290 documents with an average of 200 pages per document.
- 4.8 A vast amount officer time is spent on these requests to balance the volume against the statutory deadline. Each request has to be dealt with on a case by case basis in accordance with Data Protection Act 1998 and ICO guidance. Social cares files often include graphic content around physical, mental and sexual abuse. When considering the time required to read through such content it is clear that this can be an unpleasant exercise for Officers.

Data Protection – Data Handling

- 4.9 No organisation handling information can guarantee it will never experience losses. But the public has a right to expect that the council achieves and maintains a high standard in how it handles personal data. The Council must be effective in how it meets those expectations. Every loss or near miss must make us more determined. However, the task of improving information security will always be a continuing process.
- 4.10 The Council takes its responsibility for information security very seriously. In 2012, it agreed to a consensual audit by the Information Commissioner's Office (ICO) of its processing of personal data. An action plan was produced based on the recommendations made by the ICO. One of the key areas was mandatory training for staff on information governance and data protection.

- 4.11 Over the past 2 years, the Information Governance Team has seen an increase in the number of reported data handling incidents. We have no reason of pinpointing why this may be the case. However, it could be one or a combination of the following:
- The culture of the authority has changed to encourage people to come forward and report data handling incidents
 - There has been an actual increase in data handling issues
 - Increased training has led to increased awareness of data protection issues and the need to report them

All incidents are logged and the risks associated with the incident are assessed. Where necessary, incidents are referred to the appropriate department to investigate. The Head of Governance and Assurance investigates those incidents that are perceived to be a high risk. The Council's Senior Information Risk Officer is made aware of all incidents and he reports these through to Chief Officer Group. The annual report in Appendix 2 gives a breakdown of all data handling incidents.

Information Governance Policies

- 4.12 A key component for a robust Information Governance framework is documented policies and procedures. The Council's suite of information governance policies set out the scope and intent. Strategies, policies and guidance will be written to cover all aspects of Information Governance and Information Security as required by legislation and national guidance. These will be supplemented as a result of new developments in legal or good practice requirements or in response to identified risks or incidents within the Council.
- 4.13 The existence of up to date Information Governance policies is vital for the Council to be able to demonstrate compliance as required by the Department of Health with its information governance standards via the NHS Information Governance toolkit. This is vital for both Public Health and Social Care, as without it they will not be able to access NHS data to perform their tasks.
- 4.14 Information Governance policies will typically be written by the Information Governance team or the Director of Digital Services (also the Council's Senior Information Risk Owner), circulated to the IG Board for comment and agreement, and then formally approved by the Personnel Committee and the Corporate Joint Committee. Approved policies will be published on the Council's Intranet site (iDerby) and where appropriate on the Council's web site. Policies will be reassessed, amended and approved on an annual basis. Where there are any significant changes in organisational arrangements, or the underlying legislation or national guidance has changed, then the review of the relevant policies will be brought forward.

Records Management

- 4.15 Good records management is essential for the Council to function effectively. Records management is the systematic control of an organisation's records, throughout their life cycle, in order to meet operational business needs and statutory and financial requirements. Effective management of corporate information allows fast, accurate and reliable access to records, ensuring the timely destruction of redundant information and the identification and protection of vital and historically important records.
- 4.16 Information is every organisation's most basic and essential asset, and in common with any other business asset, recorded information requires effective management. Records management ensures information can be accessed easily, can be destroyed routinely when no longer needed, and enables organisations not only to function on a day to day basis, but also to fulfil legal and financial requirements.
- 4.17 The main area for attention in 2015 was to review and update the Council's Records Retention Schedule. A complete review of the Council's records management framework is planned to commence in 2016.

OTHER OPTIONS CONSIDERED

5.1 None.

This report has been approved by the following officers:

Legal officer	n/a
Financial officer	n/a
Human Resources officer	n/a
Estates/Property officer	n/a
Service Director(s)	n/a
Other(s)	n/a

For more information contact:	Richard Boneham Head of Governance and Assurance, 01332 643280 richard.boneham@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 – Implications Appendix 2 – Information Governance Annual Report 2015

IMPLICATIONS

Financial and Value for Money

1.1 None directly arising.

Legal

2.1 None directly arising.

Personnel

3.1 None directly arising.

IT

4.1 None directly arising

Equalities Impact

5.1 None directly arising.

Health and Safety

6.1 None directly arising.

Environmental Sustainability

7.1 None directly arising.

Asset Management

8.1 None directly arising.

Risk Management

9.1 Sound risk management practices are a key principle of good information governance.

Corporate objectives and priorities for change

10.1 The governance framework includes arrangements to plan and monitor delivery of the Council's priorities.

