Derby City Council

Audit and Accounts Committee
30 January 2018

ITEM 7

Report of the Director of Information Services

Information Assurance Update

SUMMARY

1.1 This report provides Members of the Committee with an update on information management arrangements across the Council.

1.2 Detailed performance reports are presented every six months and the next full report is scheduled for May 2018. This interim report gives a short update on activity since November 2017 with a particular focus on GDPR preparations.

RECOMMENDATION

2.1 To note the report.

2.2 To request a further Information Assurance update in May 2018.

REASONS FOR RECOMMENDATION

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.

3.2 The Council holds a considerable amount of confidential and sensitive information. It is essential that this information is managed properly.

SUPPORTING INFORMATION

4.1 This update report covers the following areas:

- Freedom of Information Act 2000 / Environmental Information Regulations 2004
- Data Protection Act 1998 – Subject Access Requests
- Information Security
- Preparation for the General Data Protection Regulations 2016 (GDPR)
- Other

4.2 **Freedom of Information (FoI) /Environmental Information Regulations (EIR) Requests**

4.3 The Council is currently responding to 78% of requests within the statutory 20 days against an annual target of 94%. This target was based on last year's performance and set before the introduction of a senior management sign-off process. The Information Commissioner's Office expect a minimum performance of 90%.

4.4 A number of procedural changes have been adopted over the last six months to improve performance, most recently the introduction of a weekly email to Directors that lists all requests due within the following 10 days. Complex requests, requiring input from a number of different divisions, are now coordinated by the Information Governance (IG) team with sign off by the Interim Director of IT (previously each section was required to secure separate sign off). These changes are already having a positive impact although it will be difficult to recover the 2017/18 performance so late in the year.

4.5 **Data Protection Act 1998**

Overall performance is 89% against an annual target of 80%. This is a significant improvement on the 2016/17 performance of only 30% and thanks to changing working practices and the considerable efforts of the team.

4.7 **Information Security**

Departments continue to report a high level of security incidents to the Council's IG team. Four incidents were reported to the ICO in 2017 - all have been closed by the ICO without further action.

4.8 The new post of Information Security Officer has been filled and the new post-holder will start with the Council on February 1st. His immediate priorities will be to review the Council's Information Security Policy and Incident Reporting and Investigation arrangements and to instigate a programme of corporate awareness. Another early priority is a review of the Council's IT account management processes.

4.9 **GDPR Preparations**

The new General Data Protection Regulations (GDPR) come in to effect on the 25th May 2018. GDPR replaces the existing Data Protection Act 1998. The primary objective is to give individuals greater control and increased rights in relation to personal data.

4.10 A task and finish (T&F) group has been established to oversee the Council's preparations. The group meets monthly. The group reports to the corporate Information Governance Board chaired by the Interim Director IT (and SIRO). Paragraph 8.3 describes some of the work of the project to date.

4.11 **Roles and responsibilities**

The Council depends on a range of key IT business systems in its day to day operations e.g. Oracle Finance and Liquid Logic. These systems often hold highly sensitive and confidential data. It is important that everyone involved in the management of these systems is clear about who is ultimately responsible for the integrity of the systems and for the security and quality of the data they hold. The responsibilities for key information governance roles have been properly defined and signed off by departmental management teams. These include Information Asset Owners. Systems Owners and Asset Administrators.

4.12 **Data Mapping**

The regulation imposes much higher compliance obligations so we need to have a very good understanding the data assets we hold and how they are managed and used. One of the key activities has been a fundamental refresh of the Council's Information Asset Inventory – this is our point of reference for locating data and ensuring there are clear points of contact and accountability.

4.13 **Retention**

The IG team, the IT business application support teams and the T&F representatives have agreed a corporate retention and disposal schedule which is another fundamental compliance requirement.

4.14 **Disposal**

The Head of Transformation and Business Application Support, IT Services, is leading a project to apply the retention and disposal schedule to the Council's IT systems starting with a selection of key 'gold' applications.

4.15 **Awareness Programme**

The IG team are working closely with corporate communications to deliver the GDPR awareness programme. Updates are being delivered through InTouch bulletins; manager bulletins; manager briefings; AV screens and iDerby pages.

4.16 **Statutory Deadlines**

The Regulations introduce;

- mandatory information security breach reporting; the ICO must be notified within 72 hours of the Council becoming aware of a breach
- a reduced time frame for processing subject access requests; previously 40 calendar now to be one calendar month
- new rights to be processed in one calendar month, such as; rectification, erasure portability, prevention and objection of processing

As a result of these new obligations the IG team have been and will continue to undertake policy amendments, creation of procedures, and formulation of guidance and production of templates. These changes will place much higher obligations on corporate resources; specifically the Information Governance team.

4.17 **Other**

Surveillance

Surveillance concerns the use of personal data, and is therefore governed by privacy legislation.

A centrally held corporate surveillance inventory has been completed by all applicable services to ensure that we are able to track and locate all the relevant assets, and are aware of the Asset Owners. The Council's Surveillance Policy clearly defines roles and responsibilities and mandates self-assessment to meet compliance obligations.

The Information Governance team play an active role in advising on daily surveillance

issues, these include but aren't limited to; lawful bases, information sharing, police disclosures, privacy impact assessments, pixelation, deployments etc.

4.18 **Sold service**

The IG Team offer a sold service to both LA maintained schools and academies. The service encompasses FOI advice, Data Protection advice and preparation for the GDPR. Considerable training and support is provided to the schools.

South Derbyshire District Council has recently procured the IG Team's support in preparing for the GDPR. The service encompasses the work set out at 8.3 on a smaller scale. Further interest has been shown for a 'business as usual' Information Governance sold service, and proposal has been offered.

OTHER OPTIONS CONSIDERED

5.1 N/A

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:	Jill Craig jill.craig@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 – Implication

IMPLICATIONS

Financial and Value for Money

1.1 None directly arising.

Legal

2.1 None directly arising from the report.

Personnel

3.1 None directly arising.

IT

4.1 None directly arising

Equalities Impact

5.1 Data Protection also includes sensitive equality information and so it is essential that we are able to do all we can do to prevent any breaches.

Health and Safety

6.1 None directly arising

Environmental Sustainability

7.1 None directly arising

Property and Asset Management

8.1 None directly arising

Risk Management

9.1 Non-compliance with FOI and Data Protection legislation opens up the risk that the Council attracts a monetary penalty or other sanctions from the ICO. This is particularly important going forward as from the 25th May 2018 when the General Data Protection Regulations (GDPR) come into force the penalties for non-compliance can be up to 4% of worldwide turnover or 20 million Euros, whichever is higher. Information risks are monitored on a regular basis by the Interim Director, Jill Craig.

Corporate objectives and priorities for change

10.1 The functions of the Committee have been established to support delivery of corporate objectives by enhancing scrutiny of various aspects of the Council's controls and governance arrangements.