AUDIT & ACCOUNTS COMMITTEE
19 June 2018

Report of the Interim Strategic Director, Resources

ITEM 17

Information Assurance Update

SUMMARY

1.1 To provide Members of the Committee with an update on information management arrangements across the Council.

RECOMMENDATION

2.1 To note the report and to

2.2 request a further Information Assurance update in December 2018.

2.3 approve the consolidation of various existing policies into a single Information Security and IT Acceptable Use Policy.

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 vast amount of confidential and sensitive information. It is essential that this information is managed properly.

3.3 Consolidating a number of related often overlapping policies in to a single document reduces confusion and simplifies policy management.

SUPPORTING INFORMATION

4.1 This report provides an update across the following areas:

- The Council's adoption of the General Data Protection Regulations (GDPR)/Data Protection Act 2018;
- 2017/18 performance: Requests for information under the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Data Protection Act 1998;
- Information Security;
- Other information management improvement activity.

5 The Council's adoption of the General Data Protection Regulations /Data Protection Act 2018

5.1 In accordance with General Data Protection Regulations (GDPR) the UK's new Data Protection Act 2018 came in to effect on 23 May 2018. The DPA 2018 replaces the existing Data Protection Act 1998. The new legislation places greater obligations on Data Controllers and gives individuals greater control and increased rights in relation to how personal data is used.

5.2 A task and finish group was set up to oversee the Council's preparations for GDPR. The group is still meeting monthly and has been reporting to the Corporate Information Governance Board chaired by the Interim Director IT, IG and Customer Management and Strategic Information Risk Officer (SIRO).

5.3 As a result of our GDPR/ DPA 2018 preparations, the Council now has a much better corporate picture of what information it holds, what it is used for, who it is shared with and how long it should be retained. Key policies and procedures have been refreshed and Privacy Notices have been updated across all service areas. There is now a much greater awareness of the need to be transparent in how we manage personal data. Privacy Impact Assessments are now routinely carried out as part of any major change involving the storage and/or use of personal data.

5.4 The Information Commissioner has been very clear that the 25 May deadline date represented the beginning of a journey and not the end: the programme of work to ensure that we are properly managing the data entrusted to us as a public body will continue.

5.5 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.

These changes will place much higher obligations on corporate resources; specifically the Information Governance team and the impact will be closely monitored and reported to the Committee via these regular updates.

5.6 The Council's Data Protection Officer, who was also the GDPR/DPA 2018 Project Lead, will monitor on-going compliance with DPA 2018 and work with services to ensure they continue to improve their business practices.

6 2017/18 performance: Requests for information under the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Data Protection Act 1998

6.1 The following table shows the Council's performance in responding to Freedom of Information and Environmental Information requests in the last five years. (Note: since

2017/18 we have consolidated FOI/EIR performance – retaining separate statistics added no value).

6.2 During 2017 the Council introduced a senior officer sign-off process which created another stage in the approval process with a consequential impact on the time taken to process requests. During the year the team refined its operating model to accommodate this change, but for a number of months performance dropped significantly.

FOI/EIR performance

Year	Number Received		% responded to within statutory deadline	
	FOI	EIR	FOI	EIR
2013/14	1064	281	99%	99%
2014/15	1087	226	98%	96%
2015/16	1201	174	97%	98%
2016/17	1323	180	91%	87%
2017/18	1308		81%	
2018/18 (to 25 May)	222		90%	

6.3 The ICO expect organisations to respond to at least 90% of FOI/EIR requests within the statutory timeframe.

6.4 We are aware of two complaints to the ICO during 2017/18 about our handling of FOI/EIR. In one case the ICO upheld our decision not to disclose information, this related to request 8911 about Labour party agent moves. The other request was FOI request 9688, where we were advised to disclose area rented/rent paid out by specific bus companies based on a refined request.

6.5 The following table shows the Council's performance in responding to Subject Access Requests in the last five years.

Subject Access Requests

Year	Number received	Number completed	Requests on hold	Still in progress	% responded to within 40 days
2013/14	41	41	0	0	83%
2014/15	57	57	0	0	81%
2015/16	65	65	0	0	71 %
2016/17	82	81	0	1	30%
2017/18	79	78	3	1	91%
2018/19 (to 25th May)	7	4	4	3	75%*

*Note the 2018/19 performance is based on the 4 requests closed of those validated since the 1st April 2018, one of which was closed late.

6.5 The team worked incredibly hard in 2017/18 to both stay on top of new requests and close the SARs outstanding from 2016/17 and deserve considerable credit for their efforts doing what can be a very challenging task.

6.6 We are aware of two complaints to the ICO during 2017/18, one related to some missing handwritten notes that were not provided as part of the original SAR request, these have since been provided. The other complaint related to a SAR that was made by email directly to the HR department, which went into an individual's 'junk mail' inbox and as such was not picked up until sometime later. We have now provided the relevant documentation within the timeframe instructed by the ICO. Unfortunately we also had occasion to report a SAR related data breach to the ICO after some personal data was not correctly redacted from within a 10,000 page SAR. Lessons were learned from this incident and spot checks have been introduced before material is disclosed.

6.7 Since 2017/18 we have recorded and reported on CCTV disclosure requests.

CCTV disclosure requests

Year	Number of requests received	Number of requests refused	Number of requests refused due to expired retention period	Number of requests refused due to technical issues	Number of requests refused due to no coverage	Number of requests refused due to other/ unknown reason
2017/18	**312**	**177**	**24**	**41**	**86**	**26**

6.8 CCTV requests for images of individuals are recorded as a Subject Access Request and included in those statistics.

6.9 Other CCTV requests come from a variety of sources for example the Police; insurance companies; courts; counter terrorism agencies. Because of the variety of requests and associated variety of statutory time periods for responding it would be extremely difficult and time-consuming to monitor performance; however we usually respond within 2-3 working days but it can be as little as a few hours depending on the priority. Information/evidence needed to validate the request will depend on the nature of the request, again this varies; it may be a form of authority, it may be a Police 807 form.

7 Information Security

7.1 From April 1 2017 to March 31 2018 eight serious breaches were reportable to the Information Commissioner's Office. Five of these have been closed without further action, the remainder remain open. The number of reported breaches is a cause for concern - the majority of information security breaches can be attributed to a lack of effective training and robust policy and procedures.

7.2 Since starting in this new post on February 1, the Council's Information Security Officer, has been working closely with heads of service where data breaches have occurred to provide advice and guidance and to effect procedural change.

7.3 New and much improved mandatory e-learning which was launched on June 1 is expected to produce a reduction in actual breaches, alongside an expected increase in issues raised. This expectation is based on staff appreciation and understanding of data protection and information security and of the importance of reporting information security incidents.

7.4 The People's Directorate report the majority of incidents which is in part a reflection of the complex nature of their service and the amount of sensitive personal information that they handle, and in part a reflection of their continued dependence on paper based and manual processes. An information security improvement programme is underway and overseen by the People's IT Strategy Board and supported by £600,000 capital funding. Projects include a review of the department's key operational IT systems to improve the business process flows and the investment in mobile technology for staff to reduce their use of paper. Progress will be reported to future meetings.

7.5 We are currently reviewing the existing Information Security Policy to make it more accessible staff. Rather than producing a new Policy with new content, it is an enhanced and refreshed policy which embraces, collates and replaces the following policies:

- Information Security Policy v9.1
- Laptop, Desktop and Tablet Device Security Policy
- Email, Internet Security and Monitoring Policy
- Remote and Mobile Computing Policy
- Email and Internet User Policy
- Internet File Sharing and Collaboration Sites Policy
- Malware Prevention policy
- Network User Policy

The new policy will be titled the Information Security and IT Acceptable Use Policy.

8 Other information management improvement activity

8.1 An independent review of the Council's electronic document records management system against records management best practice standards has been commissioned and will report in July 2018. The auditors have been instructed to give particular attention on its adoption within People's.

8.2 A recent organisational review of IT Services created two new posts dedicated to supporting the Council's Information Assurance Improvement Programme: an IT Security Officer and an IT Infrastructure post responsible for managing staff access to data shares to ensure staff can only access the data they're entitled to access even when they change roles.

8.3 The IT system support teams have started a programme to apply the Council's data retention policies to the Council's IT systems. Work is initially focusing on Liquid Logic (Social Care), Revenues and Benefits, HR and Payroll and Schools. This is an on-going programme of work which will eventually cover all the Council's IT systems.

This report has been approved by the following officers:

Legal officer	N/A
Financial officer	Toni Nash

Human Resources officer	N/A
Estates/Property officer	N/A
Service Director(s)	N/A
Other(s)	Richard Boneham, Ann Webster, Mike Kay, Don McLure

For more information contact:	Jill Craig jill.craig@derby.gov.uk
Background papers:	None
List of appendices:	Appendix 1 - Implications

Appendix 1

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.