AUDIT AND ACCOUNTS COMMITTEE
7 November 2018

ITEM 11

Report of the Strategic Director of Corporate Resources

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

2.2 To request a further Information Assurance update in March 2019.

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.

SUPPORTING INFORMATION

4.1 This report provides an update across the following areas:

- The Council's continued compliance with the General Data Protection Regulations (GDPR)/Data Protection Act 2018;
- 2018/19 Performance: Requests for information under the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Data Protection Act 2018;
- Information Security;
- Other information management improvement activity.

The Council's continued compliance with 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 meet monthly and has been reporting to the Corporate Information Governance Board.

5.3 As a result of our GDPR/ DPA 2018 preparations through the task and finish group 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.

To ensure continued compliance with the new Data Protection Act going forward and build on the work of the Task and Finish Group, the Data Protection Officer has established an Information Governance Working Group. The group has representation from each service who will feedback to their respective SMT meetings on works required. Key focuses of the group include: maintenance of the information inventory, privacy notices, retention schedule and creation of the website inventory. Any topical compliance issues that arise will be also be addressed by the group.

5.4 The General Data Protection Regulations Final Audit Report, focussing on the Council's preparations to ensure compliance with the Data Protection Act 2018, has reviewed and evaluated the robustness of the arrangements in place. The summary of control assurance provided was that most of the areas reviewed were found to be adequately controlled, resulting in 'reasonable assurance'. Internal controls are being addressed to achieve the two objectives identified in the audit as moderate risk, in connection with; Security Incident Reporting Procedures and Consideration of Cyber Security Insurance Cover.

5.5 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.

2018/19 Performance: Requests for information under the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Data Protection Act 2018

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 2016 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%	
2018/19 (to September)	785		93%	

6.3 The ICO expect organisations to respond to at least 90% of FOI/EIR requests within the statutory timeframe. As is shown above, the Council's performance now exceeds this target.

6.4 The Council are aware of three complaints to the ICO during 2018/19 about our handling of FOI/EIR;

- One case relates to the treatment of a request as business as usual rather than officially logging the request. This was accepted as an error, officially responded to through the correct FOI channels, and the complaint closed. Lessons have been learned from this and briefings conducted to ensure proper assessment and logging as an FOI where appropriate.

- The other two complaints are still awaiting detail from the ICO as no case officer has been assigned yet.

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

Data Subject Rights Requests

Following the implementation of the Data Protection Act 2018, information for this financial year relates to requests submitted under all data subject rights:

- Right of access (subject access requests)
- Right to rectification
- Right to erasure
- Right to object
- Right to restrict processing
- Rights in relation to automated decision making and profiling

Any historical information relates to subject access requests only.

Year	Number verified	Number completed	Still in progress	% responded to within 40 days
2013/14	41	41	0	83%
2014/15	57	57	0	81%
2015/16	65	65	0	71 %
2016/17	82	81	1	30%
2017/18	79	78	1	91%
2018/19 (to September)	59	52	7	98%

6.6 A great deal of hard work has continued in 2018/19 to both stay on top of new requests and as the stats above show so far for 2018/19, with 98% of requests on time despite a considerable increase in demands over previous years.

6.7 We are not aware of any complaints to the ICO during 2018/19, in respect of Subject Rights Requests.

6.8 Since 2017/18 CCTV disclosure requests have been recorded and reported on;

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**
2018/19 (to Sept.)	**176**	**84**	**5**	**4**	**43**	**32**

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 response within 2-3 working days is the norm, with 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.

Information Security

7.1 From 1st April 2018 to 30th September 2018 three serious breaches were reportable to the Information Commissioner's Office. One of these has 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 and staff failing to make final checks before releasing personal data.

7.2 The Council's Information Security Officer has continued to work 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 was expected to produce a reduction in actual breaches, alongside an expected increase in issues raised. This expectation was based on staff appreciation and understanding of data protection and information security and of the importance of reporting information security incidents. A significant number of reported incidents is indicative of this position.

7.4 The People's Services 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 have reviewed the suite of information security policies. Rather than producing a new Policy with new content, we amalgamated the eight policies and produced an enhanced and refreshed policy which has been agreed at Corporate Joint Committee. The new policy is titled the Information Security and IT Acceptable Use Policy and is available on iDerby, and through the e-Learning portal.

7.6 Development of the information breach management arrangements are in train, with the information security officer working on a suite of documents to include comprehensive instructions for staff as to how a data breach should be managed and a new incident reporting form.

Other information management improvement activity

8.1 The independent report on the Council's electronic document management system has been received and a further piece of work is just starting to;

- Develop a Business Classification Scheme
- Develop Records Management and Access Control Policies.

This report should be published in January 2019.

8.2 IT Services are continuing to apply the Council's data retention policies to the Council's IT systems. Work is focusing on Liquid Logic (Social Care), Revenues and Benefits, HR and Payroll and Schools. This is an on-going programme of work which will progressively cover all the Council's IT systems.

8.3 People's Services have undertaken a review of data breaches and have developed an Information Governance Improvement Programme to help prevent a recurrence. Additional laptops have been deployed for practitioners' use; further staff training has been provided; and an amendment to the printing option on the Social Care system has been explored and planned for implementation.

8.4 Derby City Council has Cyber Essential PLUS certification, awarded June 12th 2018. This significantly exceeds mandatory requirements.

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, Don McLure

For more information contact:	Andy Brammall andy.brammall@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 Director of Digital and Customer Engagement, Andy Brammall.

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.