Derby City Council

AUDIT & ACCOUNTS COMMITTEE
27 March 2019

LATE ITEM

Report sponsor: Don McLure, Strategic Director of Corporate Resources
Report author: Andy Brammall, Director of Digital and Customer Management

Information Assurance Update

Purpose

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

Recommendations

2.1 To note the report.

2.2 To request a further Information Assurance update in March 2020.

Reasons

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 The Information Governance Working Group (IGWG), with representation from all services continue to progress IG improvement both across the Council and in-service. Progress is continuing in respect of: maintenance of the information inventory, privacy notices, retention schedule and creation of the website inventory, together with addressing any emergent issues.

The work programme has been generated based on current and very real risks to the Council. The main rationale for the website inventory was to get a clear handle on what websites and microsites the Council has to reduce cyber and other compliance risks.

In parallel to the IGWG, the Council's Data Protection Officer also chairs an information security working group. The Group is built up of information governance, IT, information and customer management colleagues. The core focus of the group is to provide a coordinated approach to cyber defence of the Council.

5.3 The Council's Deputy Data Protection Officer has recently resigned from Derby in order to take up a new role, this, together with a general rise in demand for Information Governance Support from across the Council, is placing additional pressure on the IG resources until the post is successfully recruited to.

Similarly there has been an increase in both FOR/EIR and Data Protection Requests, which continues to challenge IG resources. The team are due to start implementing digital workflow for case handling, to mitigate the increase in administrative pressures. However the short term impact is that key IG resources will be invested in tailoring systems to meet the Council's needs, this is likely to impact on our compliance rates in the interim period.

5.4 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 three years.

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.

6.3 Unfortunately due to an historical error on the FOI database, which has recently come to light, FOI/EIR performance figures have been reported as higher than they should have been. The process was allowing an extra day for responses, so a number of cases were completed on day 21 rather than day 20. This has now been corrected, but for transparency, these instances have had to be reflected in the revised performance figures.

FOI/EIR performance

Current Year to Date (1st April 2018 to 24th February 2019)

	Requests received	**Requests closed**	**Performance to date**
Communities and Place	**485**	**456**	**88%**
Corporate Core	**2**	**2**	**50%**
Corporate Resources	**476**	**445**	**92%**
People Services	**327**	**295**	**82%**
Council Wide	**43**	**37**	**86%**
TOTAL	**1333**	**1235**	**88%**

Historical Performance

Year	**Number Received**		**% responded to within statutory deadline**	
	FOI	**EIR**	**FOI**	**EIR**
2015/16	**1201**	**174**	**97%**	**98%**
2016/17	**1323**	**180**	**91%**	**87%**
2017/18	**1308**		**80%**	

6.4 The ICO expect organisations to respond to at least 90% of FOI/EIR requests within the statutory timeframe. Public authorities will now be considered for monitoring by the ICO

if fewer than 90% or responses fall within the 20 working day timescale. While the performance has fallen below this due to the correction in procure, as the Council is now working to correct deadlines, the performance should normalise at previously reported compliant levels.

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

- **Cash seizures carried out by the Council -** Complaint received due to the response to the applicant stating that the information is not held - Closed, complaint not up-held

- **Correspondence relating to child sexual exploitation and grooming gangs -** Complaint received due to section 12: exceeds appropriate limit being applied to the majority of the request - ICO decision notice received, complaint not up-held

- **Correspondence relating to child sexual exploitation and grooming gangs -** Awaiting detail of complaint from ICO.

- **Recycling processing by Contractor -** Complaint received due to regulation 12(5)(e): commercial data exemption applied to questions 5 and 6 of the request. - ICO decision notice received (Council asked to release the information, and given 35 days to consider whether to appeal). This decision is currently being considered by the Strategic Director of Communities and Place

6.6 The following table shows the Council's performance in responding to Data Subject Rights Requests in the last three 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.

Current Year to Date (1st April 2018 – 24th February 2019)

Directorate	Number of requests verified	Number closed	Performance to date
Communities and Place	9	9	100%

Corporate Core	0	0	-
Corporate Resources	19	19	100%
Peoples Services	67	61	97%
Cross Departmental	5	4	80%
TOTAL	**100**	**94**	97%

Historical Performance

Year	Number received	Number completed	% responded to within 40 days
2016/17	82	81	30%
2017/18	79	78	91%

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

Directorate	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
Communities and Place	397	150	14	4	84	48
Corporate Core	0	0	0	0	0	0
Corporate Resources	41	5	1	1	2	1
People Services	2	0	0	0	0	0
Council Wide	1	0	0	0	0	0
Other/N/A	2	1	0	0	1	0
TOTAL	**443**	**156**	**15**	**5**	**87**	**49**

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 October 2018 to March 2019 Six serious breaches were reported to the Information Commissioner's Office. One of these was a complaint by a client. Of the others, one has been closed without further action from the ICO, the remainder remain open for their decision. The number of reported breaches is a cause for concern - the majority of information security breaches can be attributed to 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. Of note is a change in the LiquidLogic system, where configuration changes made on the Adults and Children's systems in November have reduced the number of accidental breaches resulting from printed documents to zero. Collaborative working, training delivery and uptake, staff vigilance and system changes are at the root of this success.

7.3 New and much improved mandatory e-learning which was launched on June 1st 2018 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 as the number of appropriate staff undertaking GDPR and Cyber Security training in the Council reached 86% at March.

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. This is closely tied in with the Digital Workforce Programme.

7.5 Development of the information breach management arrangements continue, with the information security officer working on a suite of documents to include a comprehensive Data Breach Response Plan for IT and IG staff.

Other information management improvement activity

8.1 The independent report on the Council's electronic document management system has been reviewed and feedback / comments from the Council now being taken into account. This report makes recommendations on the Council's future approach to;

- Records Management Business Classification Scheme
- Develop Records Management Policy
- Access / Security Policies.

Once fully accepted, the report will form the basis of a Records Management implementation project which will commence during the current year.

8.2 IT Services are continuing to apply the Council's data retention policies to the Council's IT systems. This is an on-going programme of work which will progressively cover all the Council's IT systems, and is expected to be complete for the majority of systems by early August.

Financial and Value for Money issues

9.1 None directly arising.

Legal implications

10.1 None directly arising from the report.

Other significant implications

Equalities Impact

11.1 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.

Risk Management

12.1 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.

This report has been approved by the following officers:

Role	Name	Date of sign-off
Legal	N/A	
Finance	Toni Nash	
Service Director(s)	N/A	
Report sponsor		
Other(s)	Richard Boneham, Ann Webster, Mike Kay, Don McLure	

Background papers:	None
List of appendices:	None