Derby City Council

AUDIT AND ACCOUNTS COMMITTEE
25 February 2015

ITEM 10

Report of the Head of Governance & Assurance

Data Protection Update

SUMMARY

1.1 This report provides the Committee with an update on specific data protection issues.

RECOMMENDATION

2.1 To note the report.

2.2 To request that in the future an annual information governance report is produced for this Committee.

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.

SUPPORTING INFORMATION

4.1 The Data Protection Act 1998 is designed to protect personal data about living individuals (data subjects). The act also places obligations on those organisations that process personal data (data controllers). As a data controller, Derby City Council is committed to complying with the legislation by applying the principles of good information handling across all its services. Failure to comply could result in adverse publicity, damage to reputation and large financial penalties from the Information Commissioner and even criminal action.

4.2 The Council has registered its use of personal information through the notification process to the Information Commissioner's Office. We keep personal information about individuals so that we can provide the services that they need and for us to maintain a record of those services. As a local authority we need to collect, process and keep data in relation to our statutory duties.

4.3 2014 has seen a large increase in the number of potential data handling/information security issues reported to the Council's Information Governance Team. These are normally reported to this Committee on a quarterly basis in the Governance Update reports

4.4 The Information Commissioner's Office (ICO) believes that a lack of effective governance structures and training programmes significantly increases the risk of serious breaches of the Data Protection Act.

4.5 In September 2012, the Council had a "consensual" audit by the Information Commissioner's Office. The overall assessment for the Council at that point in time was that the arrangements for data protection compliance with regard to governance and controls provide only limited assurance. The ICO did identify as an area of good practice that the Council had

"a strong (data protection) governance framework in place with roles and responsibilities clearly allocated. Reporting mechanisms are in place to provide a good level of corporate oversight in relation to information governance."

One of the areas of the areas identified for improvement was around the Council's training programmes for information governance. The ICO audit concluded that the Council needed to :

"Ensure that all staff receive a basic level of data protection and information security training, which should be refreshed regularly, to demonstrate competence in processing personal data in accordance with the DPA. Further specific training should be developed for staff whose roles require more in-depth training. A centrally maintained and monitored log of training will provide assurance that all relevant staff have completed this training"

4.6 At the time of the ICO audit, the Council was in the process of implementing an eLearning package to provide mandatory data protection training for all staff. The eLearning system was fully implemented in December 2013. It contains IT and data governance policies (that require acceptance) and 2 courses - Overview of the Data Protection Act and a detailed Information Governance Course.

4.7 The current level of acceptance of policies and completion of the 2 courses is shown in the table below:

Table 1: eLearning completion:

		Policies		Data Protection		Information Governance	
	Total Users	Number completed	%	Number completed	%	Number completed	%
Adults	583	373	64	76	13	48	8
CYP	999	585	59	54	5	54	5
Neighb'ds	836	568	68	247	30	161	19
C Exec	119	89	75	50	42	50	42
Resources	793	681	86	386	49	356	45
Senior Mgt	20	11	55	9	45	5	25
Overall	**3350**	**2307**	**69**	**822**	**25**	**674**	**20**

4.8 The aim is that all staff will have completed the mandatory training by May 2015.

4.9 One noticeable change in the past 12 months has been the increase in the reporting of potential data handling/ information security incidents to the Information Governance Team. It is not clear whether this is as a direct result of the increased promotion of data protection awareness within the Council. This increase in demonstrated in Table 2 below which shows reported incidents since 2011.

Table 2 : Potential Data Handling/Information Security Incidents

Year	Potential Incidents
2011	10
2012	20
2013	25
2014	63
2015 to date	19

4.10 The breakdown of incidents by directorate for the same period is shown in Table 3 below:

Table 3: Data handling issues by Directorate

Directorate	**2011**	**2012**	**2013**	**2014**	**2015**
CYP	3	7	7	20	4
AHH	1	2	4	2	3
Resources	2	8	12	28	5
Neighbourhoods	2	3	1	7	1
Chief Executive	2	0	1	1	0
Non-Directorate	0	0	0	5	6
Total	**10**	**20**	**25**	**63**	**19**

4.11 According to its annual report 2013/14 (July 2014) complaints relating to local government's handling of data made up a "high" proportion of the work carried out by the ICO. The report found that local government made up 12% of its casework relating to data protection in 2013/14, up from 11% the previous year. The report said: "Information on the type of data breaches and the sectors in which they occur shows the high number of incidents within local government and health sectors; in particular the disclosure of personal data in error." "Local government holds particularly sensitive personal information. However the high level of security breaches show that local government has much more to do to keep the information secure," it added.

4.12 The annual report also highlights that the main area where the ICO has received most complaints is in relation to Subject Access Requests (50% of complaints). This is an area of work that is showing signs of increasing, particularly in the area of special educational needs. SARs can be complex pieces of work due to the need to redact third party personal data. Often these can involve the redacting of hundreds of documents/papers. This is a resource intensive exercise. Currently the Council has 40 working days to respond to each SAR. Table 4 below shows the level of SARs since 2009. The number of SARs received in 2014 shows an increase over previous years. It should be noted, however, that although all SARs received are logged, not all are processed. This can be due to the £10 fee or relevant identification being provided.
Table 4: Number of subject Access requests received and processed:

	2009	2010	2011	2012	2013	2104
SARs received	31	28	40	38	36	51
SARs Completed	15	30	45	52	28	55

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:	Richard Boneham, Head of Governance and Assurance, 01332 643280 richard.boneham@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

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

Property and Asset Management

8.1 Information is one of the Council's most important assets. The Council must understand this and provide proper protection against loss or damage to this key asset.

Risk Management

9.1 Although there are no risks arising directly from this report, there are a number of risks where poor information governance could give rise to serious consequences:

- Penalties for failing to comply with the Data Protection Act
- Loss of access to partners information systems needed to fulfil statutory functions due to non-compliance with their access requirements
- Loss of ability to share information with partners to manage cases and support our customers.

- Damage to reputation from negative local, regional and even national media coverage following either a major breach or a repeated number of breaches.

- Disclosure of personal information could put individuals at risk of injury, harm or other damage and be liable to identity fraud or cyber-crime

Corporate objectives and priorities for change

10.1 None directly arising