



## **Information Commissioner's Office – Audit Report**

### **SUMMARY**

- 1.1 This report provides members with the outcome of the audit by the Information Commissioner's office of the Council's data protection processes.

### **RECOMMENDATIONS**

- 2.1 To note the audit report from the Information Commissioner's Office and to seek an updates at the next Committee meeting on progress being made with the actions in Appendix A of the audit report.

### **REASON FOR RECOMMENDATIONS**

- 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 Information Commissioner's Office (ICO) carries out audits to provide larger organisations with an assessment of whether they are following good data protection practice. Section 51 (7) of the DPA contains a provision that gives the ICO power to assess any organisation's processing of personal data, with the agreement of the organisation's data controller. The audits look at whether an organisation has effective policies and procedures in place and whether they are being followed and includes recommendations from the ICO on how to improve. The Information Commissioner believes that audits play a key role in assisting organisations in understanding and meeting their personal data protection obligations. The ICO sees auditing as a constructive process with real benefits for data controllers.
- 4.2 In June, the Information Commissioner's Office visited the Council as part of an investigation into a data security breach. Following this investigation the ICO recommended that the Council received an audit of its data protection practices. This was agreed and the audit took place in September. The final report from the ICO was received on 14 November 2012. The executive summary is attached at Appendix 2.

- 4.3 The overall assessment for the Council is that the arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The scope of the audit covered 3 key areas and the individual assessments for each area are shown below:
1. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation – Reasonable assurance
  2. Records management (manual and electronic) – The processes in place for managing both manual and electronic records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records – Limited assurance
  3. Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form – Limited assurance
- 4.4 The report highlights a number of areas of good practice with the ICO stating that the Council has a strong governance framework in place with roles and responsibilities clearly allocated and the reporting mechanisms that are in place provide a good level of corporate oversight in relation to information governance.
- 4.5 The ICO have scheduled follow up audits to make sure all actions are being progressed. These will be 3 months and 6 months from the date of the report being issued (14 November 2012)

<b>OTHER OPTIONS CONSIDERED</b>
---------------------------------

5.1 None.

**This report has been approved by the following officers:**

<b>Legal officer</b>	N/A
<b>Financial officer</b>	N/A
<b>Human Resources officer</b>	N/A
<b>Service Director(s)</b>	N/A
<b>Other(s)</b>	Chief Officer Group

<b>For more information contact:</b>	Richard Boneham Head of Governance and Assurance, 01332 643280 <a href="mailto:richard.boneham@derby.gov.uk">richard.boneham@derby.gov.uk</a>
<b>Background papers:</b>	None

**List of appendices:**

Appendix 1 – Implications  
Appendix 2 – ICO report – executive summary

<b>IMPLICATIONS</b>
---------------------

**Financial and Value for Money**

1.1 None directly arising.

**Legal**

2.1 None directly arising.

**Personnel**

3.1 None directly arising.

**Equalities Impact**

4.1 None directly arising.

**Health and Safety**

5.1 None directly arising.

**Environmental Sustainability**

6.1 None directly arising.

**Asset Management**

7.1 None directly arising.

**Risk Management**

8.1 Sound risk management practices are a key principle of good governance.

**Corporate objectives and priorities for change**

9.1 The governance framework includes arrangements to plan and monitor delivery of the Council's priorities.