Derby City Council

Data protection audit report

Executive Summary
November 2012

Information Commissioner's Office

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (the DPA). Section 51 (7) of the DPA contains a provision giving the Information Commissioner power to assess any organisation's processing of personal data for the following of 'good practice', with the agreement of the data controller. This is done through a consensual audit.

1.2 The Information Commissioner's Office (ICO) sees auditing as a constructive process with real benefits for data controllers and so aims to establish a participative approach.

1.3 Derby City Council has agreed to a consensual audit by the ICO of its processing of personal data.

1.4 An introductory meeting was held on 08 August 2012 with representatives of Derby City Council to identify and discuss the scope of the audit and to agree the schedule of interviews.

2. Scope of the audit

2.1 Following pre-audit discussions with Derby City Council, it was agreed that the audit would focus on the following areas:

a. 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.

b. 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.

c. 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.

3. Audit opinion

The purpose of the audit is to provide the Information Commissioner and Derby City Council with an independent assurance of the extent to which Derby City Council, within the scope of this agreed audit is complying with the DPA.

The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Limited Assurance	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 audit has identified scope for improvement in existing arrangements and appropriate action has been agreed to reduce the risk of non-compliance. We have made one reasonable assurance and two limited assurance assessments where controls could be enhanced to address the issues.

4. Summary of audit findings

Areas of good practice

There is a strong 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.

The Council's internal audit function is utilised to provide independent assessments of the policies, processes and procedures around information governance and information security.

Comprehensive fair-processing notices are in place and work has been undertaken to ensure that data subjects are aware of what data is collected, for what purpose and to whom it may be disclosed.

Areas for improvement

The development of a record of Information Assets (Information Asset Register), linked to the retention schedule, will enable key information assets to be identified and monitored. Risks associated with those assets could then be determined and appropriate staff (Information Asset owners) given responsibility for mitigating those risks.

The introduction of Privacy Impact Assessments and embedding them into the Council's project development and system design processes will provide assurance that personal data risks have been assessed.

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.

Action is required to weed and delete data from both manual and electronic records, and to ensure that this is being carried out in line with the Council's policies and retention schedule.

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Derby City Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.