Derby City Council

Follow-up data protection audit report

Executive summary
September 2013

Information Commissioner's Office

1. Background

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.

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.

The original audit took place at Derby City Council premises on 19 – 21 September 2012 and covered Data Protection Governance, Records Management and Security of Personal Data. The ICO's overall opinion was that there was limited assurance that processes and procedures were in place and being adhered to. The ICO identified scope for improvement in existing arrangements in order to achieve the objective of compliance with the DPA.

42 recommendations were made in the original audit report. Derby City Council responded to these recommendations positively, agreeing to formally document procedures and implement further compliance measures.

The objective of a follow-up audit assessment is to provide Derby City Council and the ICO with a level of assurance that the agreed audit recommendations have been appropriately implemented to mitigate the identified risks, support compliance with data protection legislation and implement good practice.

The ICO completed a desk based follow-up in July 2013 to measure the extent to which Derby City Council had implemented the agreed recommendations and identify any subsequent change to the level of assurance previously given. This was based on a management update and supporting evidence from Derby City Council.

2. Audit opinion

Overall Conclusion	
Reasonable assurance	Based on the implementation of the agreed recommendations made in the original audit report, the ICO considers that the arrangements now in place provide a reasonable assurance that processes and procedures to mitigate the risks of non-compliance with DPA are in place. The current position is summarised as three reasonable assurance assessments which shows an improvement from the original one reasonable and two limited assurance assessments in November 2012.

3. Summary of follow-up audit findings

Areas of good practice

The Council have finalised the policy documents that make up their information governance framework and have developed a policy template to ensure that any policy documents that are created in future are consistent. The Council have developed a system to provide oversight and assurance that staff have read and understood all key policy documents.

The Council have developed a number of processes to manage and monitor 3rd party contract arrangements that involve the processing of the Council's data. These include the development of Data Processing Agreement templates which are used to ensure consistency. The resulting agreements are logged and monitored by the Council's Information Governance Manager.

The Council have improved controls in relation to their off-site storage arrangements. Regular spot-checks of the off-site facility are being undertaken and procedures are in place to ensure the security of records while they are awaiting collection. Additionally, procedures have been developed for tracking files that have been retrieved from storage, to ensure that they are returned in a timely fashion.

The Council have developed a Remote Working Policy which highlights the need for information security. They have developed technical solutions to allow remote workers to access key business systems without personal data leaving the Council's network.

Areas for improvement

More work is required to develop a complete Information Asset Register that identifies and risk assesses information assets and assigns responsibility for those assets to suitable Information Asset Owners.

The Council have developed a corporate Records Retention Schedule. Work is now required to roll out similar schedules, at a local level, to individual departments and to ensure that the necessary weeding and disposal is carried out. On-going work to develop disposal logs linked to the new EDRMS system will assist in this regard.

Further work is required in relation to producing comprehensive movers and leavers processes to ensure that network and system access permissions are up-to-date and appropriate.

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.

Appendix – Original Audit Report – November 2012

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.