Doncaster Metropolitan Borough Council

Follow-up data protection audit report

Executive summary
December 2013

Information Commissioner's Office

1. Background

The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (DPA). Section 51(7) of the DPA provides the Information Commissioner with the power to assess, with the agreement of the data controller, the processing of personal data for the following of good practice. This is achieved 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 Doncaster Metropolitan Borough Council's (the 'Council') premises from the 4 – 6 December 2012 and comprised a review of Training and Awareness, Records Management and Information Sharing within selected business areas. The ICO's overall opinion was one of limited assurance that effective controls and processes were in operation, and identified scope for improvement.

34 recommendations were made in the original audit report. The Council was positive in its management response, and agreed to implement appropriate controls and processes to achieve the identified improvements.

The objective of a follow-up review is to provide the ICO with a level of assurance that the agreed audit recommendations have been appropriately implemented to minimise identified risks, and support compliance with the DPA and good practice standards.

The ICO completed a desk-based follow-up review in November 2013 to assess the progress made by the Council in implementing the agreed recommendations. The review was based on a management update and supporting evidence provided by the Council.

2. Audit opinion

Overall Conclusion	
Reasonable assurance	Based on the progress made in implementing the agreed recommendations made in the original audit report, the ICO considers that the arrangements now in place provide an overall reasonable assurance that controls and processes are in operation to minimise the risks of non-compliance with the DPA. The current position is summarised as 3 reasonable assurance assessments, which shows an improvement from the original assessments of 2 limited assurance and 1 reasonable assessment in February 2013. The follow-up review confirmed that, in our view, 19 actions are complete, 14 are in progress and 1 is incomplete.

3. Summary of follow-up audit findings

Areas of good practice

An SIRO Information Governance Board (SIGB) has been formally established, with Terms of Reference adopted and signed off by the Board. The group, who meet quarterly, has members from each Directorate and a wide remit to ensure Data Protection and Information Governance is applied consistently throughout the Council.

Mandatory online Data Protection training is now 'live' and this is supplemented by additional Information Governance training modules, including Records Management. The training, which is monitored for uptake, includes 'knowledge checks' to ensure the subject has been fully understood. Classroom based training is also made available for staff without access to computers.

The Council have developed an overarching Records Management (RM) policy to ensure RM roles and responsibilities are clearly defined and understood. The policy also defines KPIs for measuring performance of the RM function together with a clear reporting mechanism.

Processes and procedures around the Council's management of Information Sharing Agreements have been improved. This includes more training for staff drafting them, a review of existing agreements and a central log developed to allow corporate oversight.

Areas for improvement

The Council have appointed senior staff to be Information Asset Owners who are accountable for data held within their departments. However, additional work is required to populate the corporate Information Asset Register with all the Council's information assets, both electronic and paper-based, and complete appropriate training and risk assessments.

An urgent review of premises holding manual personal data is required to provide assurance to the Council that these records are held securely, environmentally controlled and comply with the Council's record's retention schedules. It is also important to ensure that as redundant premises are vacated there is corporate oversight of the disposal or transfer of records to new premises and that this is monitored.

Further work is required on local computer drives holding personal data to reduce duplicated and redundant data to ensure the Council is complying with its retention and disposal schedules.

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 Doncaster Metropolitan Borough 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.

Doncaster Metropolitan Borough Council

Data protection audit report

Executive summary
February 2013

2. 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.

Doncaster Metropolitan Borough Council (DMBC) accepted the ICO's invite to undergo a consensual audit by the ICO of its processing of personal data.

DMBC were in the process of consolidating staff into a new Civic Building during this audit. The auditors recognise that 'new ways of working' in one location will help the compliance work of the Information Governance team.

An introductory teleconference was held in October 2012 with representatives of DMBC to identify and discuss the scope of the audit and after there were further discussions in November to agree the schedule of interviews.

4. Scope of the audit

Following pre-audit discussions with Doncaster Metropolitan Borough Council (DMBC), it was agreed that the audit would be limited to Adults Social Care (Safeguarding), Human Resources and Finance (Revenue and Benefits) services and focus on the following areas:

a. Training and awareness – The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

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. Data sharing - The design and operation of controls to ensure the sharing of personal data complies with the principles of the Data Protection Act 1998 and the good practice recommendations set out in the Information Commissioner's Data Sharing Code of Practice.

5. Audit opinion

The purpose of the audit is to provide the Information Commissioner and Doncaster Council with an independent assurance of the extent to which Doncaster 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. We have made one reasonable assurance and two limited assurance assessments of scope areas where controls could be enhanced to address the issues.

4. Summary of audit findings

Areas of good practice

The DPO provides face to face training to key staff, develops e-learning and coordinates the activity of the data protection leads tasked with raising awareness in their own areas.

There are Lead Data Protection Officers, spread across all Directorates, who help raise awareness of data protection and communicate key messages.

Areas for improvement

There is currently no requirement for mandatory refresher data protection training and monitoring of training is limited.

There are no Terms of Reference for the SIRO's Information Governance Board and there is no corporate governance framework for Records Management, and as such no clear line of responsibility from the Board down for records management issues.

Records management controls require considerable development. Information Asset Owners are in place but are not yet supported by staff in the business with identifying and risk assessing the information assets held within their departments and recording these on information asset registers. In addition there is no records management policy and no procedures to ensure files removed from storage are tracked and returned promptly when no longer required.

The Council do not have an overarching data sharing protocol or policy that details when and how they will share data and there is no person or persons with oversight of the sharing taking place.
