Leeds City Council

Data protection audit report

Executive summary
November 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.

Leeds City Council were the subject of ICO enforcement action in 2012 with both an Undertaking and a Civil Monetary Penalty issued for separate data protection breaches.

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

An introductory meeting was held on 25 June 2013 with representatives of Leeds City Council to identify and discuss the scope of the audit and after that through email and telephone correspondence to agree the schedule of interviews.

2. Scope of the audit

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

a. Records management (manual and electronic) including Adults and Children's Social Services – 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.

b. 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

Overall Conclusion	
Reasonable assurance	There is a reasonable level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the Data Protection Act. We have made two reasonable assurance assessments where controls could be enhanced to address the issues which are summarised below.

4. Summary of audit findings

Areas of good practice

The Council have a robust management structure in place to coordinate Information Governance (IG) across the Council. A trained Senior Information Risk Officer is in post and there is an established Information Governance Management Board (IGMB) to provide an oversight of IG policies and procedures. Four sub-boards, with information assurance as part of their remit, report into the IGMB.

There is a clear reporting mechanism within directorates for both data protection and IT breaches. The IG manager is responsible for oversight of the directorate breach logs and will work with directorates to identify trends, record lessons learnt and formulate good practice. An annual breach report is provided to the SIRO.

The Council is compliant with CESG's Code of Connection requirements, which allows them to connect to the GCSx network. They also align their IT infrastructure to comply with other recognised standards including ISO 27001 information security requirements and the NHS' self-assessment IG toolkit.

The Council has an appropriate fair processing notice (FPN) in use within both children's and adults social services which clearly explains how it obtains, holds, uses and discloses personal data. A generic FPN is available on the Council's website and it is reviewing all data collection forms to ensure they contain a consistent FPN.

Areas for improvement

Information Asset Owners (IAOs) are not systematically assessing risk to information in their business areas, which may result in the SIRO not having an accurate overview of information risk across the Council. IAOs should regularly review the electronic and manual data they own to ensure they are clear about the nature of the information held, how it is used and transferred and who has access to it and why.

The off-site storage of manual records, including transport and retrieval, is well managed with a clear audit trail. However, there is no standardised procedure for ensuring social work case files, taken from individual offices on an ad-hoc basis, are recorded and monitored.

Implementing a single Council-wide process for storage and disposal of confidential waste will help to provide assurance that waste is being managed securely. This should include a review of the type of office shredders being used to ensure they shred to required standards.

The introduction of robust Privacy Impact Assessments and embedding them into the Council's project development and system design processes will help provide assurance that personal data risks are being assessed when new systems processing personal data are developed and implemented.

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 Leeds 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.