

City of York Council

Data protection audit report

Executive summary
November 2015

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 After two offers of a data protection audit by ICO Good Practice and following a data protection breach, a further offer by the ICO Enforcement Department, City of York Council (CYC) agreed to a consensual audit by the ICO of its processing of personal data.
- 1.4 An introductory telephone conference was held on 12th June 2015 with representatives of CYC to identify and discuss the scope of the audit and after that on 30th July 2015 to agree the schedule of interviews.

2. Scope of the audit

- 2.1 Following pre-audit discussions with CYC, it was agreed that the audit would focus on the following areas:
- a. 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.
 - b. Subject access requests - The procedures in operation for recognising and responding to individuals' requests for access to their personal data.
 - 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.
- 2.2 The audit included visits to the adult and children's social care departments, plus other relevant teams or individuals identified by CYC, in line with the agreed scope areas.
- 2.3 The audit scope areas were chosen to reflect levels of risk agreed mutually between CYC and the ICO. CYC agreed for the ICO to audit areas where it was known that improvements could be made or where processes were in transition in order for the audit to be mutually beneficial.

3. Audit opinion

Overall Conclusion	
Limited assurance	<p>There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA.</p> <p>We have made limited assurance assessments across all three scope areas: records management; subject access requests; and data sharing where controls could be enhanced to address the issues summarised below and presented fully in the 'detailed findings' and 'action plan'.</p>

4. Summary of audit findings

Areas of good practice

Policy compliance software has been implemented and was reported to be working effectively to communicate key policies to staff and ensure that they have read them.

Secure storage facilities and thorough archive procedures were in place at Yorkcraft.

Quarterly information security checks are carried out at the council's two main offices and formal audit reports are produced and presented to the Corporate Information Governance Group (CIGG).

The MAISP is a good model for Information Sharing Agreements (ISAs) because it is a high level agreement setting out common rules to be followed by all partners and is intended to be used as a basis for future ISAs.

Areas for improvement

Many services did not have up-to-date retention schedules and many staff seemed unsure about who was responsible for monitoring retention periods.

Records management does not currently feature regularly on the CIGG agenda to mandate and monitor records management improvements.

CYC is in a transitional period in relation to its SARs processes and therefore many new procedures need to be formally documented and embedded.

SARs compliance rates between 1st April 2014 and 31st March 2015 were very low, at 51.1%.

There is no systematic data sharing training in place and no council wide information governance training needs analysis to identify the requirement for such training.

CYC's PIA process is yet to be fully 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 City of York 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.