City of York Council

Follow-up data protection audit report

Information Commissioner's Office

Auditor:	Michael Stephenson (Lead Auditor)
Data controller contacts:	Lorraine Lunt (Information Governance and Feedback Team Manager)
Distribution:	Lorraine Lunt (Information Governance and Feedback Team Manager)
Date issued:	**02 June 2016**

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.

Contents

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 The original audit took place at City of York Council's (CYC) premises on 18-20 August 2015 and covered records management, subject access requests and data sharing. 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 considerable scope for improvement in existing arrangements in order to achieve the objective of compliance with the DPA.

1.4 90 recommendations were made in the original audit report. CYC responded to these recommendations positively, agreeing to formally document procedures and implement further compliance measures.

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

1.6 A desk based follow-up took place in June 2016 to provide the ICO and CYC with a measure of the extent to which CYC had implemented the agreed recommendations. This was based on management updates from CYC signed off at Board Level.

2. Follow-up audit conclusion

Scope area	**Number of recommendations in each scope area from the original audit report**	**Number of actions complete, partially complete and not implemented.**
Records Management	**41**	**13** Complete **27** Partially complete **1** Not implemented
Subject Access Requests	**25**	**6** Complete **19** Partially complete **0** Not implemented
Data Sharing	**24**	**12** Complete **12** Partially complete **0** Not implemented

Section 3 below summarises the main findings of this review and highlights any residual high risk areas.

3. Summary of follow-up audit findings

3.1 CYC has partially completed the majority of recommendations made by the ICO. Whilst it is disappointing that CYC has not completed more recommendations within the agreed timescales, it would appear that many recommendations will be completed in the next 3 months.

3.2 Senior management have recently approved a new project management approach that incorporates privacy impact assessments.

3.3 CYC have introduced a tracing system to ensure that services actively manage the whereabouts of records retrieved from storage.

3.4 27 of the 41 records management recommendations are partially complete. In multiple cases the non-completion of the recommendation is partially or wholly attributed to the need to complete a review of the records management policy. Therefore, the review of the records management policy should be prioritized to allow other recommendations to be completed.

3.5 19 of the 25 subject access requests recommendations are partially complete. In multiple cases the non-completion of the recommendation is partially or wholly attributed to the need to complete a review of the subject access request process. Therefore, the review of the subject access request process should be prioritized to allow other recommendations to be completed.

3.6 Any queries regarding this report should be directed to, Michael Stephenson Lead Auditor.

3.7 Thanks are given to the Information Governance and Feedback Team Manager who was instrumental in providing the information to complete the follow-up audit.