Sheffield City Council

Follow-up data protection audit report

Auditors:	Alexandra Lamb, Lead Auditor
Data controller contacts:	John Curtis, Head of Information and Knowledge Management
Distribution:	John Curtis, Head of Information and Knowledge Management
Date issued:	**31 March 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 Sheffield 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.

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 Sheffield City Council's (SCC) premises between 17-19 March 2015 and covered freedom of information requests, 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 69 recommendations were made in the original audit report. SCC 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 March 2016 to provide the ICO and SCC with a measure of the extent to which SCC had implemented the agreed recommendations. This was based on management updates from SCC 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.
Freedom of Information requests	**19**	**14** Complete **5** Partially complete **0** Not implemented
Subject Access Requests	**28**	**19** Complete **9** Partially complete **0** Not implemented
Data Sharing	**22**	**5** Complete **17** 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 The auditor was pleased to note significant progress across freedom of information and subject access scope areas and was encouraged by the evidence that SCC volunteered to support the improvements detailed in its Action Plan. Areas where improvements are particularly noteworthy include:

- A target of 95% has been approved by the Information Governance Board (IGB) to respond to FOI requests within the required time frame.
- FOI compliance statistics now form part of IGB's standard agenda.
- Quality assurance is carried out on FOI requests to ensure the correct dates are being recorded.
- A Standard Operating Procedure (SOP) has been amended to explain how SCC deals with FOI requests involving partner organisations.
- SAR guidance has been added to SCC's website and a direct link to the guidance is presented prominently on the homepage.
- Template letters and guidance have been published on the intranet for staff to use when responding to SAR's to ensure consistency.
- SAR compliance statistics now form part of the IGB's standard agenda.
- SCC has ensured that the Centre for Excellence data sharing template will be promoted for use with all new data sharing arrangements.
- The minimum security standards that need to be adopted for the transfer of records in an information sharing agreement have now been documented.

3.2 The ICO recommends that SCC's commitment to completion of the Action Plan continues to ensure that all risks identified in the audit are mitigated as far as possible. Priority should be given to the data sharing scope because a number of these recommendations have only been partially completed. We have also highlighted some other areas that SCC should consider giving priority to:

- Implementing new training for SCC staff in relation to recognising an FOI request, staff responsible for responding to FOI requests, FOI portfolio representatives, SIRO's and senior members of SCC.
- Updating e-learning training to bring it in line with current SOP requirements.
- Reviewing contracts with partner organisations to ensure that there are appropriate clauses in place to allow proper processing of FOI requests.
- Reviewing existing contracts with data processors to ensure that a SAR handling clause is inserted.
- Completing regular quality assessments of SAR's to ensure that information has been withheld correctly.
- Updating SCC's Information Asset Register (IAR) and assigning owners to information assets.
- Finalising the data sharing policy.
- Recording the nature and justification of sharing personal data as recommended.
- Recording the relevant exemptions or conditions for processing personal data within information sharing agreements.
- Completing a training needs analysis to identify staff that require specialised training in information sharing.
- Incorporating security incident procedures into data sharing policies.
- Ensuring that one off disclosures of personal information are logged as recommended.
- Ensuring quality checks are carried out to assess the appropriateness of one off disclosures.

3.3 It was also noted that a target of 85% for SAR completion has been accepted the by the IGB, however, the ICO recommends that the SAR completion target should be at least 95%. This would also bring SCC's SAR completion target in line with their FOI target of 95%.

3.4 The management response summary confirms SCC's commitment to appropriate completion of all actions.

3.5 Any queries regarding this report should be directed to Alexandra Lamb, Lead Auditor.

3.6 Thanks are given to John Curtis, Head of Information and Knowledge Management who was instrumental in providing the information to complete the follow-up audit.