Coventry City Council

Data protection audit report

Executive summary
February 2018

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.

The ICO originally conducted a consensual audit of Coventry City Council (CCC) during 13-15 October 2015, which covered data protection governance, training and awareness and data sharing. The ICO published and concluded in the corresponding audit report that there was a very limited level of assurance that effective processes and procedures were in place and delivering adequate data protection compliance at CCC.

As a result, CCC agreed during August 2016 to undertake a second consensual ICO audit in respect of their processing of personal data.

An introductory teleconference was held on 15 September 2017 with representatives of CCC to identify and discuss the scope of the audit, and after that on 4 October 2017 to agree the schedule of interviews.

The audit field work was undertaken at Friargate during 21-22 November 2017.

2. Scope of the audit

Following pre-audit discussions with CCC, it was agreed that the audit would focus on the following areas:

a. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

b. 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.

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

3. Audit approach

The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk based review of selected policies and procedures, onsite visits including interviews with selected staff, and an inspection of selected records.

The purpose of the audit was to provide the Information Commissioner and CCC with an independent assurance of the extent to which CCC, within the scope of this agreed audit, is complying with the DPA.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with the DPA.

In order to assist data controllers in implementing the recommendations, each has been assigned a priority rating based upon the risks that they are intended to address. These ratings are assigned based on the following risk matrix:

Impact					
	Severe	High	High	Urgent	Urgent
	High	Medium	Medium	High	Urgent
	Medium	Low	Medium	Medium	High
	Low	Low	Low	Medium	High
		Remote	Unlikely	Likely	Very Likely
		Likelihood			

It is important to note that the above ratings are assigned based upon the ICO's assessment of the risks involved. CCC's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

4. Audit opinion

The purpose of the audit is to provide the Information Commissioner and CCC with an independent assurance of the extent to which CCC, within the scope of this agreed audit, is complying with the DPA.

Overall Conclusion	
Limited assurance	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. We have made two limited assurance assessments in relation to data protection governance and data sharing, and one reasonable assurance assessment in relation to training and awareness, where controls could be enhanced to address the issues which are summarised below.

5. Summary of recommendations

Urgent Priority Recommendations – These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of the DPA.	We have made **13** urgent priority recommendations across all 3 scope areas: **8** in data protection governance; **1** in training and awareness; and **4** in data sharing, where controls could be enhanced to address the issues identified.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of the DPA.	We have made **41** high priority recommendations across all 3 scope areas: **18** in data protection governance; **7** in training and awareness; and **16** in data sharing, where controls could be enhanced to address the issues identified.
Medium Priority Recommendations - These recommendations address risks which can be tackled over a longer timeframe or where mitigating controls are already in place, but which could be enhanced.	We have made **69** medium priority recommendations across all 3 scope areas: **38** in data protection governance; **23** in training and awareness; and **8** in data sharing, where controls could be enhanced to address the issues identified.
Low Priority Recommendations - These recommendations represent enhancements to existing good practice or where we are recommending that the data controller sees existing plans through to completion.	We have made **18** low priority recommendations across all 3 scope areas: **9** in data protection governance; **7** in training and awareness; and **2** in data sharing, and where controls could be enhanced to address the issues identified.

6. Summary of audit findings

Areas of good practice

The Information Governance Annual Report records the number of information security incidents in comparison with those for the previous financial year, the number and outcomes of incidents reported to the ICO, a breakdown of incidents by risk classification and type, and examples of ICO Civil Monetary Penalties issued to other councils, in order to facilitate associated trend analysis and lesson learning.

The Information Governance Dashboard records completion of the mandatory e-learning and alternative classroom training for monitoring purposes; this information is refreshed weekly.

CCC utilise the Data Sharing Register to prompt and log reviews of data sharing agreements.

Areas for improvement

Information risk management is underdeveloped at CCC; there is no dedicated group to monitor risk, there is no formal link between incident management and privacy impact assessments and overarching risk registers, there are no Directorate or Service Risk Registers to facilitate the escalation of risks from operational level, the Information Risk Management Policy does not adequately cover data processors and there have been no risk assessments to date in respect of information assets.

There are no formal documented Key Performance Indicators to assist CCC in gauging and driving data protection compliance.

There is no documented data protection training strategy and the training needs analysis has not been subject to formal approval.

There is neither a formal approval process, nor a central register, of fair processing notices.

Data sharing agreements do not consistently specify how or when relevant parties should notify CCC of an information security incident.

Data sharing agreements do not require all parties to notify each other when personal data are amended or updated, and CCC do not obtain assurance in regard to the secure disposal of shared data at the end of defined retention periods.

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 Coventry 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.