

# Coventry City Council

## Data protection audit report

Executive summary  
March 2016

## 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 invited Coventry City Council to participate in a Data Protection Audit in January 2015.

In February 2015, Coventry City Council agreed to a consensual audit by the ICO of its processing of personal data.

An introductory meeting was held on 06 August 2015 with representatives of Coventry City Council to identify and discuss the scope of the audit.

Prior to the audit, the Council recognised opportunities to improve on the existing information governance framework. Via its Information Management Strategy Group attended by the SIRO and other senior managers it had developed a number of plans to improve practice to promote data protection compliance.

At the time of the audit, as part of the plans for improvement referred to above, the Council's Information Governance Team was undergoing a period of change with a number of roles within the team that were vacant following a restructure. Interviews were ongoing to recruit new staff to this team including a Senior Information Governance Officer.

## 2. Scope of the audit

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

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.

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.

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.

### 3. Audit opinion

<b>Overall Conclusion</b>	
<b>Very Limited assurance</b>	<p>There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.</p> <p>We have made two very limited and one limited assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report.</p>

## 4. Summary of audit findings

### **Areas of good practice**

Key information governance related policies are in place including a Data Protection Policy, an Information Security Policy and a Records Management Policy which are available on the intranet for staff to access. In addition, a new suite of guidance has been produced which the Council has named the "Information Toolkit." Although these documents are yet to be finalised, a communications campaign is planned to launch the new toolkit to staff.

The induction checklist requires new staff to read the Data Protection Policy and they are required to sign to say that they have done so.

### **Areas for improvement**

The Council is reported to be currently taking a different strategic direction in regards to information governance as a whole. At the time of the audit however, there was no operational lead (data protection officer) or supporting staff (other than one information governance officer) in place to monitor data protection compliance and promote improvement, although the Council is currently running a recruitment campaign.

Information Asset Owners (IAOs) have yet to be formally identified and the role and responsibilities of IAOs have not been formally documented e.g. within a role description. Also, the Council has not documented a consistent and cohesive approach to the management of information risk within a formal policy or created a stand-alone information risk register. Neither does the information asset register appear to be used to facilitate the assessment and management of relevant risks. As a result, information risk is not managed in a structured way to ensure that senior management is fully aware of the risks to personal data and can ensure they are assessed and mitigated appropriately.

Data protection related training has been mandatory for all staff within the Council since November 2014 but is still in the process of being rolled out across the organisation. Training completion statistics are not regularly reported to the Information Management Steering Group (IMSG) to ensure that training is being completed by new starters at the beginning of their employment, to monitor training completion across the organisation and to identify where improvement is needed. In addition, the Council does not provide specific training for specialised roles or

functions such as IAOs, Subject Access Request handlers and staff involved with data sharing.

There is insufficient clarity around who has corporate responsibility for ensuring that data sharing takes place appropriately. In addition, there are currently no published policies or guidance which clearly define systematic data sharing and one-off requests for disclosure, who has the authority to make decisions about them and when it is appropriate to do so.

---

**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.**