Shropshire Council

Data Protection Audit

Follow-Up Review

Executive Summary

July 2012

1. Background to follow-up assessment

1.1 The Information Commissioner may, with the consent of the data controller, assess the extent to which good practice is applied when processing personal data and shall inform the data controller of the results of the assessment. (Data Protection Act (DPA) 1998 s51, (7))

1.2 The Information Commissioner sees auditing as a constructive process with real benefits for data controllers and so aims to establish, wherever possible, a participative approach. (Assessment Notice Code of Practice 2.1)

1.3 An Assessment Notice is the medium through which the Information Commissioner's Office (ICO) will seek to instigate a compulsory audit. However, the Assessment Notice Code of Practice, in the interests of clarity, distinguishes between compulsory and consensual audits. (Assessment Notices Code of Practice, 2.1, Para 6 & Appendix A.)

1.4 The audit took place at Shropshire Council's (SC's) premises in Shrewsbury and Market Drayton in September 2010. Its overall conclusion was of 'Reasonable Assurance' that processes and procedures are in place and being adhered to. The ICO identified some scope for improvement in existing arrangements in order to achieve the objective of compliance with the Data Protection Act 1998.

1.5 Thirteen recommendations were made in the original audit report. The Council responded to these recommendations positively, agreeing to formally document procedures and implement further compliance measures.

1.6 The desk based follow-up took place in April 2012 and this review was arranged to provide the ICO with a measure of the extent to which the Council had implemented the agreed recommendations and identify any subsequent change to the level of assurance previously given.

2. Follow-up audit approach

2.1 When undertaking a follow-up assessment the objective is to provide the Information Commissioner with a level of assurance that the agreed audit recommendations have been appropriately implemented to mitigate the identified risks and support compliance with data protection legislation.

2.2 The original audit gave the Council an overall opinion of 'Reasonable Assurance' and thirteen recommendations were made.

2.3 The follow-up comprised a desk based assessment of documentary evidence supplied by the Council in support of the implementation of the agreed recommendations.

3. Follow-up audit opinion

Overall Conclusion	
High Assurance	Based on the implementation of the agreed recommendations made in the original audit report ICO Audit considers that the arrangements now in place still provide a high assurance that processes and procedures to mitigate the risks of non-compliance with DPA are in place. The current position is summarised as thirteen high assurance assessments which shows improvement from the original assessments of six limited and seven reasonable assurance assessments in October 2010. The 'detailed findings and action plan' at Section 6 of this audit report shows the current position with regard to the implementation of the agreed recommendations.

4. Summary of follow-up audit findings

4.1. SC has made improvements to its project management methodology so that all new proposals are subject to a PIA process.

4.2. Improvements have been made to the movers and leavers process so as to provide more effective controls.

4.3. The county's SOPHOS application is now being employed to provide effective endpoint control over devices such as memory sticks as well as checking software patches and updates.

4.4. Significant improvements have been made to the homeworking process to ensure teleworking complies with overall security policy.

4.5. New systems and processes have been adopted for social care records management covering areas including file tracking.

4.6. SC have now fully implemented the transformation project designed to move staff paper records to electronic format and which covers related retention times.

Shropshire Council

Data Protection Audit Report

Executive Summary
October 2010

Auditors:	Kai Winterbottom	- Team Manager (Audit)
	David Simmons	- Engagement Lead Auditor
	Chris Littler	- Auditor

Distribution:

Draft Report: Ceri Pilawski, Head of Audit Services
Roy Morris, Information Governance Officer

Summary Report: Kim Ryley, Chief Executive
Ceri Pilawski, Head of Audit Services

Report Issued: 29 October 2010

1. Background

1.1 The Information Commissioner may with the consent of the data controller assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment. (DPA s51, 7)

1.2 In September 2009 Shropshire Council informed the Information Commissioner of a loss of personal data contained on a password protected but unencrypted USB memory stick. This device contained a complete copy of one of the Social Care databases and was sent by post to a contractor in Cardiff by post. The letter in which the device was enclosed was damaged in transit and the USB stick was lost.

1.2 Following investigations into this incident by ICO Enforcement staff, it was agreed that Shropshire Council would sign an official Undertaking. This required Shropshire Council to comply with various requirements including controls on storage and transfers of personal data, data encryption of portable electronic storage devices, security and other checks on third party data processors and adequate training for staff dealing with personal data.

1.3 The Shropshire Council undertaking was signed in December 2009 but in March 2010 the Council reported another security breach to the Information Commissioner, this time involving Criminal Record Bureau request paper files. The actual loss occurred prior to the signing of the Undertaking and therefore was not considered a formal breach of the undertaking but was again grounds for investigation by ICO Enforcement.

1.4 Senior Council executives met with ICO Enforcement staff to discuss DPA non-compliance issues and invited the ICO to Audit DPA related procedures so as to identify areas for improvement and advice on good practice.

1.5 An introductory meeting was held on the 23 July 2010 with Shropshire Council to establish an appropriate scope for an audit and it was agreed to assess Council procedures and working practices relevant to the reported data losses.

2. Audit Scope

The audit scope focused on specific processes and activities in relation to subject access requests, to assess how their implementation contributes to compliance with the data protection principles within the following areas:

Data protection governance within Shropshire Council with reference to its procedures, statements of internal controls, risk management strategy and risk registers.

Processes and procedures to manage the collection, access, content and movement of electronic personal data within and between county offices. Processes and procedures implemented, to appropriately secure such personal data held by Shropshire Council.

Processes and procedures to manage the secure processing and movement of personal data, both manual and electronic, with reference to staff working from home or otherwise away from the office. This to include the effectiveness of the methods used to develop and maintain data protection awareness by staff within the identified directorates.

Processes and procedures to manage the secure processing and movement of personal data, both manual and electronic, between council premises and third party processors including CRB.

Records management policies and procedures for the weeding and retention of personal data throughout council departments

3. Overall Opinion Audit

3.1 On the basis of the work performed, the ICO considers that the current arrangements in place at Shropshire Council, with regard to data protection governance and effective data security, provide a reasonable assurance that processes and procedures are in place and being adhered to. Some improvements in procedures are however recommended to help ensure full compliance with all Data Protection Act 1998 requirements.

3.2 Shropshire Council have undertaken major projects to establish common systems and procedures following the creation of the new Unitary body and have introduced uniform electronic data processing based around a new central data centre. However, there are still areas for improvement relating to risks associated with the processing of paper records including the need for improved and uniform security procedures.

3.3 We have made one limited assurance and four reasonable assurance assessments where controls could be introduced or existing controls improved to address the issues identified in the report. Shropshire Council has submitted a positive action plan to improve their controls which builds on the improvements they were already making.

Overall Conclusion	
Reasonable Assurance	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified areas of good practice, some scope for improvement in existing arrangements, and appropriate action needs to be taken to enhance the likelihood that the objective of data protection compliance will be achieved.

4. Summary of Audit Findings

4.1 Shropshire Council employees generally have a good understanding of DPA principles and how these should be applied to work practices as a result of mandatory training and key message delivery via the eShrop intranet.

4.2 The council has invested in records management systems to cover both paper and electronic records to improve tracking and data management capabilities.

4.3 Privacy Impact assessments and check lists are being introduced to help identify any data protection risks associated with new personal data handling systems.

4.4 A new network 'end point' control system is being introduced to audit and control the use of devices such as USB memory sticks.

4.5 The council has introduced a new secure system for CRB request transfers but this is not being used universally.

4.6 Council policy requires confidential information to be destroyed securely but inconsistent standards are being applied to the storage of confidential waste and the security of paper files and cupboard key storage.

4.7 There is no reliable system in place to monitor the removal and return of paper files containing personal data from departments sampled.

4.8 Whist the council has a home worker agreement it was unclear whether all staff working at home have been asked to read and sign it. Staff awareness of personal data security should be reinforced as part of this process.