Northumberland County Council

Follow-up data protection audit report

Executive summary
September 2013

1. Background

1.1 The Information Commissioner is responsible for enforcing and promoting compliance with the Data Protection Act 1998 (DPA). Section 51(7) of the DPA provides the Information Commissioner with the power to assess, with the agreement of the data controller, the processing of personal data for the following of good practice. This is achieved 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 Northumberland County Council's (the 'Council') premises from the 31 July – 2 August 2012 and comprised a review of Training and Awareness, Security of Personal Data and Requests for Personal Data (SARs) within selected business areas. The ICO's overall opinion was one of limited assurance that effective controls and processes were in operation, and identified scope for improvement.

1.4 52 recommendations were made in the original audit report. The Council was positive in its management response, and agreed to implement appropriate controls and processes to achieve the identified improvements.

1.5 The objective of a follow-up review is to provide the ICO with a level of assurance that the agreed audit recommendations have been appropriately implemented to minimise identified risks, and support compliance with the DPA and good practice standards.

1.6 The ICO completed a desk-based follow-up review in September 2013 to assess the progress made by the Council in implementing the agreed recommendations. The review was based on a management update and supporting evidence provided by the Council.

2. Audit opinion

Overall Conclusion	
Reasonable Assurance	Based on the progress made in implementing the agreed recommendations made in the original audit report, the ICO considers that the arrangements now in place provide an overall reasonable assurance that controls and processes are in operation to minimise the risks of non-compliance with the DPA. The current position is summarised as 1 high assurance and 2 reasonable assurance assessments, which shows an improvement from the original assessments of 2 limited assurance and 1 reasonable assessments in September 2012. The follow-up review confirmed that, in our view, 26 actions are complete, 22 are in progress and 4 are incomplete.

3. Summary of follow-up audit findings

Progress Made against Action Plan

An Information Security Working Group has been formally established, with Terms of Reference agreed and signed off at senior level. The group, who meet fortnightly, has members from each Directorate and a wide remit to ensure Data Protection and Information Governance is applied consistently throughout the Council.

The Council's suite of Information Governance polices have been reviewed and refreshed. Procedures have been put in place to automatically flag-up policies to their owners when they are due for review.

Mandatory online Data Protection training has now gone 'live' and this is being supplemented by additional Information Governance training modules. The training, which is monitored for uptake, includes 'knowledge checks' to ensure the subject has been fully understood.

Processes and procedures around the Council's management of Subject Access Requests have been improved to include robust monitoring and reporting of KPIs to senior management.

Further Work Required

Further development of an Information Asset Register, together with an associated information risk assessment, is required.

The Homeworking policy is still being drafted. It is essential for homeworkers to know and understand the Council's recommended practices and procedures to ensure the security of personal data while working from home.

Additional training for Information Asset Owners is still required in order for them to understand the specialist nature of the role in helping the Council comply with the DPA.

More work is required at the Council's records archive, along with a revised Data Retention Policy to ensure paper records are disposed of in line with agreed retention schedules.

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 Northumberland County 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.

Northumberland County Council

Data protection audit report

Executive summary
October 2012

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 Audit is the result of three security breaches reported by the Northumberland County Council (the Council) to the ICO in June and July 2011:

1) Case reference ENF0393260 involved the theft of a memory stick containing some 540 employees' pension information.

2) Case reference ENF0404181 involved the release of two medical assessments to the wrong parties.

3) Case reference ENF0407334 involved a child assessment report being sent to the wrong individual.

A subsequent investigation by our Enforcement Team recommended the Council should take advantage of the ICO's audit service in order to assist them in ensuring future compliance with the DPA.

1.4 The Council has agreed to a consensual audit by the ICO of its processing of personal data.

1.5 Conference calls were held with representatives of the Council on 28 May 2012 to identify and discuss the scope of the audit and on 25 June 2012 to agree the schedule of interviews.

2. Scope of the audit

2.1 Following pre-audit discussions with Northumberland County Council it was agreed that the audit would focus on the following areas:

a. 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.

b. Security of personal data – The technical and organisational measures in place to ensure that there is adequate security over personal data held in manual or electronic form.

c. Requests for personal data – The processes in place to respond to any requests for personal data. This will include requests by individuals for copies of their data (subject access requests) as well as those made by third parties

3. Audit opinion

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

3.2 The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Limited assurance	The arrangements for data protection compliance with regard to governance and controls provide a limited assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements. We have made one reasonable assurance and two limited assurance assessments of scope areas where controls could be enhanced to address these issues.

4. Summary of audit findings

Areas of good practice

The Council have a formal IT governance framework in place, led by the Information Security Board, with the remit to oversee information security across the organisation. The Board is chaired by the Senior Information Risk Officer (SIRO).

The Council is compliant with level 4.1 of CESG's Code of Connection requirements which allows them to connect to the GCSX network. They are also implementing a major refresh of their IT infrastructure to comply with ISO 27001 information security requirements.

There is a clear reporting mechanism for data protection/IT breaches with the Information Governance Officer (IGO) responsible for collating the incidents and entering them on to the Breaches Log. IT works with line managers to identify the cause, formulate an action plan and record lessons learnt.

The Council maintains a 'white-list' of acceptable devices that can be connected to their network and non-standard devices are blocked. All USB memory sticks and laptops are encrypted and secure printing / faxing is enforced with Multi-Functional Devices requiring a user pin code to access the device.

Areas for improvement

There is no individual with oversight of data protection training to ensure training needs are assessed, training materials are adequate and mandatory training is completed by all staff.

There is no formal process to ensure staff have read and understood the Council's data protection policies and procedures and know where to locate them on the Council's intranet.

The Data Protection Working Group has day-to-day oversight of data protection but it has no terms of reference or clear reporting structure.

Information Asset Owners should regularly evaluate the electronic and manual data they own to ensure they are clear about the nature of the information held, how it is used and transferred and who has access to it and why.

Clear CCTV signage, as recommended by the ICO's CCTV Code of Practice, is not always apparent.

There is no formal procedure to ensure staff with access to applications containing sensitive data have their access rights revoked when changing departments.

The Council needs to clarify who are their Data Protection Lead Officers, formalise this part of their role and provide specialised training if required.
