Hampshire County Council

Data protection audit report

Executive summary

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.

Hampshire County Council (HCC) has agreed to a consensual audit by the ICO of its processing of personal data.

An introductory meeting was held on 28 September 2016 with representatives of HCC to identify and discuss the scope of the audit and after that on 09 November 2016 to agree the schedule of interviews.

2. Scope of the audit

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

a. Records management (manual and electronic) – The processes in place for managing both manual and electronic records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

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. 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.

3. Audit opinion

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

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

Overall Conclusion	
High Assurance	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with the DPA. We have made two high assurance ratings in relation to Training and Awareness and Security of personal data. We have made one reasonable assurance rating in relation to Records Management.

4. Summary of audit findings

Areas of good practice

- The Risk Management Board (RMB) is responsible for ensuring corporate risk is identified and managed effectively. It is chaired by the Senior Information Risk Owner (SIRO) and attended by Departmental SIROs, which are in place across HCC.

- The RMB receives reports about information risk from the Information Governance Steering Group (IGSG) which is chaired by the Deputy SIRO. Attendees include the Data Protection Officer, Departmental Data Protection Coordinators (DPCs) and representatives from the Records Management Service. Information Management Steering Groups have also been set up within Adults' Services and Legal Services.

- Information Asset Registers have been created within each Department. They are reviewed each year by the Departmental SIROs, DPCs and Information Asset Owners to ensure they remain accurate. Adults', Children's and Legal Services have retention schedules in place for all the personal data they hold.

- It is a requirement for all staff with access to HCC's IT system to complete a specific data protection e-learning training programme. The course is comprehensive and includes a test that staff must pass. Refresher training is completed annually. At the time of the audit 96% of staff with IT access had completed the training programme.

- A wide range of information security management policies and procedures are in place. The IT Policy Review Panel maintains a policy register and ensures they are regularly reviewed and updated. HCC's IT Department has held the ISO27001 Information Security Management System certification since 2008.

Areas for improvement

- There are no routine checks on the casework management systems in Adults' and Children's Services to monitor whether staff are only accessing records on a 'need to know' basis. Legal Services are unable to study a user's viewing history in their casework management system.

- Manual records out on loan from Legal/Adults'/Children's Services central storage location are not recalled after a certain period of time. There is a risk manual records could potentially be held off-site indefinitely.

- There is no process in place for ensuring that staff assigned with Mass Storage Devices, such as USB sticks, are still in possession of them.

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 Hampshire 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.