Renfrewshire Council

Follow-up data protection audit report

Executive summary
August 2013

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 original audit took place at Renfrewshire Council premises on 23-25 October 2012 and covered data protection governance, security of personal data and requests for personal data. The ICO's overall opinion was that there was reasonable assurance that processes and procedures were 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 DPA.

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

The objective of a follow-up audit assessment is to provide the ICO and Renfrewshire Council with a level of assurance that the agreed audit recommendations have been appropriately implemented to mitigate the identified risks, support compliance with data protection legislation and implement good practice.

The ICO completed a desk based follow-up in July 2013 to measure the extent to which Renfrewshire Council had implemented the agreed recommendations and identify any subsequent change to the level of assurance previously given. This was based on a management update and supporting evidence from the Council.

2. Audit opinion

Overall Conclusion	
High assurance	Based on the implementation of the agreed recommendations made in the original audit report, the ICO considers that the arrangements now in place 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 three high assurance assessments which shows an improvement from the original two reasonable and one limited assurance assessments in January 2012. The 'detailed findings and action plan' at section 5 of this report shows the current position with regard to the implementation of the agreed recommendations. The follow-up review confirmed that 14 actions were complete, with 7 ongoing/partially complete.

3. Summary of follow-up audit findings

Areas of good practice

- Reporting measures in relation to data protection have greatly improved and KPIs are now reported through the governance structure.

- Refresher training based around information security is now mandatory for all staff on an annual basis.

- Security incidents are now logged corporately.

- Third party requests for data are now recorded and reported to the SIRO on a monthly basis.

Areas for improvement

- Consider setting a more challenging completion target to ensure that all existing staff receive the online data protection/information security training as soon as possible.

- Introduce 'spot checking' to ensure that the clear desk policy is adhered to.

- Ensure that all data sharing agreements, including historical agreements, are logged centrally.

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 Renfrewshire 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.

APPENDIX – Executive Summary of HPT audit dated January 2013

Renfrewshire Council

Data protection audit report

Executive summary
January 2013

Information Commissioner's Office

2. 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.

Renfrewshire Council (RC) has agreed to a consensual audit by the ICO of its processing of personal data.

An introductory meeting was held on 13 September 2012 with representatives of RC to identify and discuss the scope of the audit.

4. Scope of the audit

Following pre-audit discussions with RC, 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.

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.

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 those made by third parties and sharing agreements.

5. Audit opinion

The purpose of the audit is to provide the Information Commissioner and RC with an independent assurance of the extent to which RC, 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	
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 some scope for improvement in existing arrangements. We have made 1 limited and 2 reasonable assurance assessments of scope areas where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' at section 7 of this report

4. Summary of audit findings

Areas of good practice

There are local risk registers in place that incorporate information risk and are used to drive the Internal Audit plan.

The Council security controls in place surrounding identity access management include complex passwords and monitoring of starters, leavers and movers.

There are appropriate network access controls in place including the encryption of mobile devices.

Data Protection Officers in each service receive additional training that includes the handling of requests.

There is a central log of SARs which includes details of key dates and who is responsible for completing the request.

Areas for improvement

There are few reporting measures in relation to data protection reported through the governance structure.

Reporting of compliance does not routinely inform the Annual Statement of Governance.

There are no corporate logs for security incidents.

There is no mandatory refresher training for data protection in place.

Third party requests are not recorded or reported corporately.

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 Renfrewshire 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.