Portsmouth City Council

Follow-Up Audit

Executive Summary

April 2012

1. Background to follow-up assessment

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))

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)

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.)

The Information Commissioner has reiterated a desire, in the first instance and as far as is practicable, to conduct consensual data protection audits.

Following the report of an inappropriate disclosure of third party data in response to an individual's subject access request the ICO served an Undertaking on Portsmouth City Council (PCC). The ICO contacted PCC to suggest that an audit of their data processing framework by the ICO may help them understand the extent to which they are complying with the DPA and to promote good practice.

Following the audit the ICO's overall conclusion was of 'reasonable assurance' that processes and procedures were in place and being adhered to. Consequently the ICO identified some scope for improvement in existing arrangements in order to achieve the objective of compliance with the DPA.

The ICO made 35 recommendations in the original audit report. PCC responded to the recommendations positively, agreeing to formally document procedures and implement further compliance measures.

This desk based follow up review was arranged to provide the ICO with a measure of the extent to which PCC had implemented the agreed recommendations and to reassess the level of assurance.

2. Follow-up scope

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

This audit assessment involved a desk based review of documentary evidence provided in relation to PCC's action plan.

The evidence reviewed included updated policies and procedures, an assessment which demonstrated implementation of 24 good practice recommendations.

3. Follow-Up Opinion

Conclusion	
Reasonable Assurance	Based on the implementation of the agreed recommendations made in the original audit report ICO Audit considers that the arrangements currently in place provide a reasonable assurance that processes and procedures to mitigate the risks of non-compliance with DPA are in place. The current position shows significant improvement. The assurance rating is summarised as three high assurance and one limited assurance assessments. This shows an improvement from the original position of one limited assurance and three reasonable assurance assessments in June 2011. The desk based review confirmed that 24 actions are complete, with five ongoing and six incomplete.

4. Summary of Follow-Up Audit Findings

Areas of good practice

Introduction of software to ensure all corporate policies have owners, are dated, regularly reviewed and delivered to every relevant officer.

Review and amendment of PCC's Data Protection Code of Practice and Information Governance Policy.

Production of quarterly compliance statistics for the Corporate Information Governance Panel.

Production of Privacy Impact Assessment guidance to ensure PCC projects involving personal data are risk assured.

Areas for improvement

An audit programme to ensure all completed documents are stored on the Electronic Social Care Record rather than on users' drives and for the removal of duplicate personal data is yet to be implemented. Compensatory manual controls implemented to minimise duplication.

While work has been commissioned there is currently no system access monitoring and reporting.

The implementation of an information asset register and data flow mapping exercise has been delayed while PCC undergoes an 18 month corporate wide transformation programme.

5. Appendix a – Executive summary of original report

Portsmouth City Council

Data Protection Audit Report

Executive Summary

1. Background

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))

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)

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.)

The Information Commissioner has reiterated a desire, in the first instance and as far as is practicable, to conduct consensual data protection audits.

Following the report of an inappropriate disclosure of third party data in response to an individual's subject access request, an Undertaking was served on Portsmouth City Council (PCC). The ICO contacted PCC to suggest that an audit of their data processing framework by the ICO may be beneficial to understand the extent to which they are complying with the DPA and to promote good practice.

PCC agreed to a consensual audit by the ICO of its processing of personal data.

An introductory meeting was held on the 11 November 2011 with representatives of PCC to identify and discuss the scope of the audit.

2. Audit Scope

Following pre-audit discussions with PCC, 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.

Training - The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.

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

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.

3. Audit Opinion

The purpose of the audit is to provide the Information Commissioner and PCC with an independent assurance of the extent to which PCC, within the scope of this agreed audit is complying with the Data Protection Act 1998 (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 and appropriate action is to be agreed to reduce the risk of non compliance. We have made one limited and three reasonable assurance assessments where controls could be enhanced to address the issues summarised below and presented fully in the 'detailed findings and action plan' of section 7 of this report along with management responses.

4. Summary of Audit Findings

Areas of Good Practice.

Policies are readily available to all staff through the intranet and can be located alphabetically, by category or using the search function.

There is a well developed and functioning information governance structure in Social Care.

There is regular liaison between the Caldicott Guardians and IGO and a monthly IG panel attended by all three where data protection issues are discussed and actions agreed.

There are departmental and corporate risk registers with individual risk owner. The corporate risk register includes the risk of theft, loss or accidental destruction of data.

There is an established procedure for dealing with requests from third parties.

Areas for Improvement.

Policies do not consistently show the date of production, last review and owner of the document. Several documents had not been developed for a number of years.

Inconsistencies between the ICT IG Strategy and the DP Code of Practice indicate a lack of a joined up approach to data protection.

There is currently no central oversight of data protection compliance level or control activity in the departments by any central committee or group.

There are very few statistics collected on PCC's compliance with the DPA 98 and no reporting of those figures to any function or group.

Information about subject access requests (SAR) and third party request are not collated corporately and used to provide PCC with an overview of their compliance although the IG team and Social Care collate their own data to measure some elements of compliance.

A review of the findings of the 2008 internal audit shows that some recommendations are still outstanding.

There is no corporate requirement for departments to undertake PIA.

There is no corporate overview of the training that is undertaken although the MLE system may allow these controls to be developed.

There was no evidence of an Information Asset Register, either for electronic records or manual records.

Retention schedules have not been adequately enforced in relation to electronic records that PCC are processing.

There is little oversight corporately of monitoring the sharing of personal data.

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 rests with the management of Portsmouth 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.