Portsmouth City Council

Follow-Up Audit Report

Final

Auditors:	Lee Taylor – Team Manager Audit Richard Ansell - Auditor
Follow-Up Report Distribution:	Peter Harding (Corporate Information Governance Officer) Helen Magri (Corporate Information Governance Officer) Angela Dryer (Caldicott Guardian) Vaughan Tudor-Williams (Caldicott Guardian) Janice Boucher (Information Governance Officer Social Care) Michael Lawther (City Solicitor/Monitoring Officer/SIRO)
Follow-Up Report Issued:	26 April 2012

Contents

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

1.5. 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.

1.6. 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.

1.7. 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.

1.8. 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 audit 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 which shows an improvement from the original position of one limited assurance and three reasonable assurance assessments in June 2011. 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. The desk based review confirmed that 24 actions are complete, with 5 ongoing and 6 incomplete.

3. Summary of follow-up audit findings

3.1 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.

3.2 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.

4. Follow-up audit approach

4.1 When undertaking a follow-up assessment the objective is to provide ICO Audit 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.

4.2 The original audit was rated as a reasonable level of assurance and 35 recommendations were made. On review the progress of the majority of the agreed actions should be assessable remotely by a desk based review. Therefore a revisit in this case was not deemed necessary and a report containing a revised assurance level was produced following an assessment of the documentary evidence provided.

5. Follow-up report grading

5.1. Follow-up audit reports are graded with an overall assurance opinion linked to the implementation of the agreed audit recommendations. The implementation or otherwise of the recommendations are classified individually to denote their relative importance, in accordance with the definitions in the table below.

Colour Code	Internal Audit Opinion	Recommendation Priority	Definitions
	High assurance	Minor points only are likely to be raised	The arrangements for data protection compliance provide a high level of assurance that processes and procedures are in place and being adhered to and that the objective of data protection compliance will be achieved. No significant improvements are required.
	Reasonable assurance	Low priority	The arrangements for data protection compliance 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 has been agreed to enhance the likelihood that the objective of data protection compliance will be achieved.
	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The achievement of the objective of data protection compliance is therefore threatened. Actions to improve the adequacy and effectiveness of data protection governance and control has been agreed and timetabled.
	Very Limited assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

6. Detailed follow-up report findings

Findings and recommendations from the previous audit have been risk categorised using the criteria defined in Section 5. The rating will take into account the impact of the risk and the probability that the risk will occur in relation to the implementation of the agreed audit recommendations.

For continuity and ease of reference, the recommendations have been numbered in line with the original report and relevant action plan responses.

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
6.1 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.				
a.	The lack of a robust and consistent governance process for evaluating the effectiveness of the application of policies and procedures for managing and processing personal data raises the risk that personal data may be processed and	A3. By ensuring policies are consistently dated, have version numbers, identify owners and have a specified review date PCC will be able to ensure staff are working from current requirements.	Action: PCC has purchased software (Conform) which will ensure all corporate policies have owners, are dated, regularly reviewed and delivered to every relevant officer. Risk-based approach to be taken to decide order in which policies are loaded. Owner: SIRO Completion date: April 2012	**Complete.**
		A4. A control list of local and corporate policies is useful to highlight review dates that	Action: See above. Conform will compile this list	**Complete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
	managed inappropriately, with the potential for damage and distress to individuals.	are due and provide a corporate overview of the policies that are available.	Owner: SIRO Completion date: April 2012	
		A6. By ensuring that the corporate IGOs are consulted where local policies are produced PCC will be able to increase their assurances that overall policy delivers compliance.	Action: All policies to be called-in and reviewed by CIGOs. Lead officers to ensure approval of any future policies in their area is sought from CIGO NB – LG to see if Conform has this functionality Owner: CIGO on behalf of SIRO Completion date: October 2011	**Complete.**
		A7. Review the Data Protection Code of Practice and the ICT IG strategy to ensure they deliver a joined up approach and reflect the current strategy for compliance in PCC.	Action: To review both policies and re-write as necessary Owner: CIGO/Head of IS on behalf of SIRO Completion date: December 2011	**Complete.**
		A13. Where there is a centralised oversight of data protection governance PCC will be able to ensure that there is suitable authority to mitigate any identified relevant risks. For example,	Action: Terms of Reference to be written for CIGP. Quarterly meetings (and in the event of a data Security breach) Owner: SIRO	**Complete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
		this could be a function of the IG group under the leadership of the SIRO.	Completion date: July 2011	
		A17. By formalising the ToR of the IG group to include reporting lines to the GAC and a work programme, PCC will be able to increase the group's ability to identify and mitigate risks.	Action: Formalise ToR to include reporting lines. Initial work programme to mirror actions within this plan Owner: SIRO Completion date: July 2011	**Complete.**
		A20. By jointly reviewing the role of the data protection coordinators and IG liaison officers PCC can reinforce the responsibilities of staff in those roles. If PCC add the consolidated and revised role to staff objectives and training they will be further able to ensure compliance and sharing good practice.	Action: Role of Lead Officers to be formalised – report to go to Strategic Directors Board for approval. Training to be delivered to Lead Officers as necessary Owner: SIRO/CIGO/IS Completion date: October 2011	The role of Information Security Champions has been approved and will be nominated to staff going forward. New/replacement Lead Officers will receive training from CIGOs. **Ongoing.**
		A24. Where the corporate IGOs are required to collate statistics on data protection compliance they will increase their overview and identification of problems early in the process.	Action: CIGOs to collate corporate statistics quarterly and report to Governance & Audit. Owner: CIGO Completion date: October 2011	**Complete**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
		A29. Further to the work commissioned by the SIRO, where PCC ensure that information risks identified are reflected in the corporate and departmental risk registers they will be able to develop a process to highlight and mitigate these risks.	Action: TBC – LG to speak to Dominic Kirby Owner: Completion date	**Complete.**
		A30. Require Director's returns that feature information risks or data protection compliance problems to be flagged to the corporate IG panel.	Action: No action deemed necessary. PCC feels this is adequately covered by measures already in place. Owner: Completion date:	Recommendation rejected originally for Directors to report on activity in their areas. PCC note that data protection issues are reported to the CIGP and the Governance & Audit Committee. **Incomplete.**
		A37. By requiring departments to conduct PIAs when undertaking projects involving personal data PCC can increase their assurance that risks are identified and reduced.	Action: CIGO to liaise with Paul Summers (Corporate Programme Manager) to ensure PIAs are conducted in relation to all new projects. Owner: CIGO/Corporate Programme Manger Completion date: September 2011	**Complete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
6.2 Training - The provision and monitoring of staff data protection training and the awareness of data protection requirements relating to their roles and responsibilities.				
b.	A failure to provide and implement staff training and awareness regarding the processing of personal data raises the risk of loss or inappropriate use of data, with the potential to cause damage and distress to individuals, and reputational damage to Portsmouth CC.	B2a. By regularly reviewing the Induction Process Policy Statement PCC will be able to bring this up to date with current good practice and incorporate any changes in guidance.	Action: Review the policy and update as necessary Owner: HR Completion date: October 2011	**Complete.**
		B2b. Where staff are made aware of the requirements for handling personal data PCC increase their assurance of complying with the requirements of data protection.	Action: Healthcheck to be mandatory across the authority and certificate renewed every 2 years. Content to be Managers to have responsibility for ensuring their team complete the Healthcheck and enrol on any further training as a result. Content of Healthcheck to be reviewed/refreshed as necessary before each roll-out. Continue to use existing induction training options Owner: HR/CIGO Completion date: December 2011	**Complete.**
		B4. As each department carries out its own IG training it is imperative that	Action: This is only correct of Social Care – all other services use the corporate training	**Complete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
		corporate IG ensure that a consistent message is being communicated to staff in each department.	packages. HR already working with Social Care to ensure consistency. The Healthcheck can be adapted and used on an ongoing basis Owner: HR/IGO for SC Completion date: October 2011	
		B5. A review of training methodology for IG in departments would enable good practice to be established and a consistent approach developed across PCC. This would enable a consistent level of knowledge on handling personal data to be embedded.	Action: As for B4 Owner: HR/CIGO Completion date: December 2011	**Complete.**
		B7. PCC require a method of refresher training to be implemented that would ensure all staff receive up-to-date information on handling personal data. IG should have extensive input to the training detail and receive information regarding the extent to which all appropriate staff	Action: The CIGO will continue to have input into all IG training developed by HR. As for B4 Owner: HR/CIGO Completion date: December 2011	**Complete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
		has been trained.		
		B8. Roll-out of the refresher training test and course should be completed as soon as possible and made mandatory for all those who process personal data.	Action: As for B3 Owner: HR/CIGO Completion date: December 2011	**Complete.**
		B10. By ensuring that Corporate IG obtains figures on completion of IG training they will be able to target training needs	Action: HR to provide report to CIGO showing officers who have completed/not completed training. CIGO to pursue through managers. Owner: HR/CIGO Completion date: December 2011	**Complete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
6.3 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.				
c.	A failure to appropriately maintain control over personal data records raises the risk it may be inaccurate, incomplete, inadequate, or mislaid. It may also be inappropriately disclosed, resulting in distress to affected individuals, non-compliance with the DPA and reputational damage to Portsmouth CC.	C4. Scanned documents containing personal data that might be retained on user's drives are still subject to data protection requirements. There is a risk that documents left on user's drives will not be processed in line with data protection. By producing and reviewing reports of documents that are not deleted by the system PCC will be able to take action to mitigate any risks by making individuals aware of the need to delete documents once they have been added to ESCR.	Action: To develop and review current processes for deletion of duplicate information. Produce procedures for staff on compliance with process. Raise staff awareness of the requirement to delete duplicate records that are no longer necessary and especially not on their own drives. Owner: Angela Dryer – Caldicott Guardian and Social Care IG Panel Chair Completion date: September 2011	Partially rolled out in social care. Outstanding proposal for automated deletion of client records from staff U drives etc when indexing onto ESCR. **Ongoing.**
		C16. The inclusion of these records in any Information Asset Register that is created will help to ensure that they are subject to the requirements to process them inline with data protection and PCC policy.	Action: Ascertain how much data is stored on the 'W' Drive and link into C4 to develop and review process for staff, raise awareness of not saving to personal drives. Also links into work on corporate Information Asset Register. • Part 1 – How much data is	Guidance and training provided to ensure all completed documents are stored on the ESCR. Audit programme to be established to ensure compliance and remove all duplicate data. Compensatory manual controls implemented to minimise duplication. **Incomplete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
			stored on 'W' Drive and develop and review process. • Part 2 - Link in to Corporate Information Asset Register • Part 3 - Recommendations to be made by Caldicott Guardian for Children's Services Owner: Initially Angela Dryer – Caldicott Guardian Chair of the IG Panel then Caldicott Guardian for Children's when known. Completion date: Unable to determine until corporate IAR is in place	
		C19. By implementing a retention schedule for these records PCC will ensure they are processed inline with their requirements under data protection.	Action: Clarify with other LAs retention period for Safeguarding files where there has been a Safeguarding investigation. Owner: IGO for SC Completion date: September 2011	**Complete.**
		C24. Where access to systems is monitored PCC	Action: This issue is in hand and will be ongoing. We will need to	There is currently no system access monitoring and reporting but

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
		reduce the risk that personal data will be obtained unlawfully. Introducing audits once the Business Objects software licences are introduced will aid with this monitoring.	wait for change in hosting arrangements for SWIFT to be fully implemented before routine audits can be introduced. Owner: Angela Dryer – Caldicott Guardian and Chair of the Social Care IG Panel Completion date: November 2011	negotiations are ongoing with system supplier to enable this functionality. **Incomplete.**
		C26. Data surrounding records management, in relation to the destruction and archiving of records, reported into the IG structure (for example, the Corporate IG Panel), can be used to help PCC maintain an oversight of their information requirements.	Action: (Social Care)JB to speak with Jim Lines and the MIOs to see current reports generated and how we can use them in respect of Records Management. Aim would be to routinely use these reports to ensure figures are reported into the IG Structure both within Social Care and corporately. (Corporately) John Shurvinton to be invited to join the CIGP. Owner: IGO for SC/IS (Records Management) Completion date: September 2011	No mention of production of management statistics to the CIGP on the weeding, destruction and archiving activity in services. **Incomplete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
		C28. An IAR allows IG an overview of the personal data that they process and provides an assurance that the processing is done in line with the DPA.	Action: IARs are a requirement of the Information Governance Toolkit for Social Care but a more comprehensive Corporate IAR is required.IAR to be compiled authority-wide using template provided by IS Owner: SIRO (but owner for each area will be asset owner) Completion date: December 2012	PCC is undergoing a Corporate Wide Transformation programme over 18 months. During this period an IAR will be developed. PCC has acknowledged this as an ongoing risk. **Ongoing.**
		C29. As the SWIFT system is phased out there is an opportunity to ensure that the new system adheres to PCC's retention policies.	Action: This work has already been highlighted and will be addressed when hosting of SWIFT changes in the Autumn. Owner: Angela Dryer – Caldicott Guardian and Chair of the Social Care IG Panel Completion date: Initial work expected to commence October/November 2011	Swift records due for deletion are identified by regular report to IS which deletes the records. No mention of new system. **Ongoing.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
6.4 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				
d.	A failure to appropriately manage and process subject access requests raises the risk of non-compliance with the DPA causing damage and distress to individuals and reputational damage to Portsmouth CC.	D3. If the corporate IG team formalise their procedures for dealing with requests for personal data they will have greater controls in maintaining complaint standards	Action: Develop written procedures Owner: CIGO Completion date: July 2011	**Complete.**
		D5. By consulting with other departments in PCC that handle requests the corporate IGOs will be able to ensure consistency and share good practice when formalising its procedures.	Action: Social Care to share their newly revised process. To include as an agenda item on next Lead Officer meeting to discuss Owner: CIGO Completion date: July 2011	**Complete.**
		D9. Where multiple logs are used to manage and record requests the use of an accurate due date in all logs will offer assurance that requests are dealt with in line with the DPA.	Action: No action deemed necessary. Manual logs only used temporarily as a workflow aide – RESPOND to be used to monitor due dates Owner: Completion date:	**Complete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
		D10a. Where PCC develop a single standard system (incorporating the good practices from the existing processes) for each department handling requests to use they would be better placed to produce an aggregated view of their compliance rates, identify any non compliance and improve consistent handling of requests	Action: CIGO to complete analysis with Education/Housing to establish feasibility of all DSAR requests received in these areas being logged/handled by the Corporate Information Governance Team. Owner: CIGO Completion date: August 2011	**Complete.**
		D10b. Where request handlers compile and report compliance statistics to a central person or body (see recommendation A6) there will be a better oversight of the level of PCC's compliance. (see recommendation A8). Any causes of overdue requests can then be addressed.	Action: CIGO to collate statistics for authority quarterly and report to SIRO/Governance & Audit. Owner: CIGO Completion date: September 2011	**Complete.**
		D13. By rolling out the electronic redaction tool to other departments PCC will be able to ensure a consistent approach to dealing with requests.	Action: No action deemed necessary. CIGOs/IGO/Request Handlers in Social Care already have tool. Not deemed necessary for Housing/Education as typically	PCC deemed no action necessary at the time but note that electronic redaction is used in the areas where it is needed. **Incomplete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
			entire file is available for inspection with very little redaction required. Owner: Completion date:	
		D17. Ensure that there are up to date data sharing protocols in place for all routine sharing of personal data outside of PCC and that they identify the owner, the data to be shared and a date for review.	Action: All protocols to be called-in/reviewed/adapted as necessary to provide a uniform approach across the authority. Owner: CIGO/Relevant Service Completion date: December 2011	**Complete.**
		D18. Assign high level responsibility for the oversight of information sharing to a single person or body to keep the list under review and ensure that protocols are in place and up to date.	Action: To be reviewed routinely by CIGP, overseen by SIRO. LG to investigate whether CONFORM would have functionality to assist in this task Owner: SIRO/CIGO Completion date: November 2011	Information Sharing Protocols are brought before CIGP as the authorising body. **Complete.**

Ref	Compliance Risk	Recommended Solution	Management Comments, Responsibility for Action and Due Date (as of report dated 23 June 2011)	Current Position at time of follow up review (March 2012)
		D21. The experience of the Social Care Department presents an opportunity to feed into a dataflow mapping exercise to compile a list of all data flows out of PCC. This will allow greater awareness and control of personal data that is shared with other organisations.	Action: Data Flow Mapping Exercise to be carried out as part of review of Protocols/Information Asset Register. Social Care to share knowledge. Owner: CIGO/IS Completion date: December 2011	PCC is undergoing a Corporate Wide Transformation programme over 18 months. During this period data mapping and data flow lists will be developed. PCC acknowledges the risk in this approach. **Incomplete.**

6.5 Any queries regarding this report should be directed to Richard Ansell, ICO audit.

6.6 Thanks are given to Peter Harding and Helen Magri who were instrumental in providing the information to complete this desk based assessment and coordinating the onsite review.