Item 7.1

Cardiff Council

Data protection audit report

Executive summary
June 2014

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 ICO issued Cardiff Council with an Undertaking in August 2013 and consequently the Council agreed to implement processes to ensure it processed personal data in accordance with principle 7 of the DPA. Following this, the ICO asked the Council to consider a consensual data protection audit.

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

An introductory teleconference was held on 4 March 2014 with representatives of Cardiff Council to identify and discuss the scope of the audit and after that on 1 April 2014 to agree the schedule of interviews.

2. Scope of the audit

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

a. 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.

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 Cardiff Council with an independent assurance of the extent to which Cardiff Council 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	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non compliance with the DPA. We have made three reasonable assurance assessments where controls could be enhanced to address the issues which are summarised below.

4. Summary of audit findings

Areas of good practice

The Council have a robust management structure in place to coordinate Data Protection and Information Governance across the Council. This comprises of a Senior Information Risk Officer (SIRO), a Data Protection Officer, Information Governance (IG) Manager and an IT Security Officer (ITSO), who report in to an established Information Security Board.

A series of e-learning modules covering data protection and IT security have been rolled out to staff. Completion of these is monitored by the Improvement and Information Management Team (I&IM Team) and reminders sent to managers if staff fail to complete them. Additional modules have also been developed for staff with specialist roles, for example staff who deal with Subject Access Requests.

There is a clear reporting mechanism within directorates for both data protection and IT breaches. The IG Manager is responsible for oversight of the directorate breach logs and will work with directorates to identify trends, record lessons learnt and formulate good practice. Regular breach reports are provided to the Information Security Board.

The ITSO is a member of the local WARP (Warning, Advice, and Reporting Points) programme. This is part of the Information Sharing Strategy of the Centre for the Protection of National Infrastructure (CPNI) and provides IT security advice at a local level.

The Council is compliant with PSN's robust Code of Connection requirements, which allows them to connect to the PSN network. They also align their IT infrastructure to comply with other industry standards including ISO 27001 and the Information Technology Infrastructure Library (ITIL). These frameworks ensure information security management is an integral function of the Council's IT service delivery.

Privacy Impact Assessments (PIAs) are mandatory for every new project, or any significant change to, systems which process personal data. These requirements are documented in the Project Quality Assurance process and guidance on how to complete PIAs is available to project management staff. PIAs are recorded in a log and the progress of the PIA is regularly monitored.

Areas for improvement

Information Asset Owners (IAOs) are not systematically assessing risk to information held in their business areas, which may result in the SIRO not having an accurate overview of information risk across the Council. IAOs

should regularly review 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.

There is no corporate Information Asset Register to ensure the Council has a mechanism for understanding and managing risks to their information. It should link information assets to dependencies including risk assessments, retention schedules and owners. The register should be maintained and regularly updated, with a named owner responsible for overseeing this.

Several of the Council's IT related policies were overdue for review at the time of audit. It is good practice to review policies on an annual basis in order to ensure that policy information for staff is relevant and kept up-to-date.

The Council is rolling out refresher data protection refresher training for managers but do not have plans to update all Council staff with regular data protection refresher training once the current series of e-learning modules have been completed.

Physical security can be enhanced by implementing a single Council-wide process for storage and disposal of confidential waste. This will help provide assurance that waste is being managed securely and should include a review of the type of containers being used to store confidential waste before disposal.

Appendix A

Detailed findings and action plan for Cardiff Council.

Action plan and progress

Recommendation	Agreed action, date and owner	Progress at 6 months
Data Protection Governance		
A1. Ensure the cover sheet of the Information Governance Strategy is updated to reflect that has been approved by Cabinet.	Accept – Strategy cover sheet updated to reflect approval Implementation Date: Immediate Owner: Information Governance Manager	
A2. Ensure the Information Management Strategy is ratified and approved as soon as possible and this is communicated to relevant staff.	Accept - IMS to be approved by Information Security Board on 2nd July and put onto Forward Plan for Cabinet Approval Implementation Date: July 2014 Owner: OM, Improvement & Information	
A4. Ensure that all	Accept –	

IG/DP policies remain up-to-date and fit for purpose by reviewing them at least annually. Also ensure they have a standardised cover sheet that shows their accountable owner, approval body and the date for review.	RM Policy and IT Security Policies to be reviewed in September 2014 both will be reviewed and owned by Information Security Board. Implementation Date: September 2014 Owner: Information Governance Manager & ICT Security & Compliance Manager	
A9. Ensure suitable IAO training is provided to IAOs ensure they are fully conversant with their role and what it entails.	Accept – Gradual training to be introduced as part of the introduction of the Information Security Service Risk Register. Formal training to be provided October 2014 Implementation Date: October 2014 Owner: Information Governance Manager	
A13. Ensure all outstanding recommendations contained in the Welsh Audit Office reports are implemented within the required timescales.	Accept – Outstanding recommendations will be actioned as required in line with the AGW's Reports Implementation Date:	

	Immediate Owner: OM, Improvement & Information	
A16. The IG risk register should be submitted to the Information Security Board for sign-off and incorporated into Council procedure to inform the Corporate Risk Register process.	Accept – The IG Service Risk Register will be submitted to ISB for sign off and fully operational by each IAO by beginning of Quarter 3 2014/15. Implementation Date: October 2014 Owner: Information Governance Manager & Data Protection Officer	
A17. Implement local IARs, maintained by IAO's, that feed into a Corporate IAR. A Corporate IAR could then be used to help inform risks on the Information risk register.	Accept – Following successful implementation of IG Service Risk Registers the Council will conduct an assessment in line with the National Archives IAR template to ascertain if any additional assets are required to be captured and maintained as part of each IAO's Risk Register Implementation Date: October 2014	

	Owner: Information Governance Manager & Data Protection Officer	
A18. Consider the inclusion of a data protection compliance audit within the Council's 2014-2015 internal audit plan.	Accept – Internal Audit will investigate conducting elements of DPA compliance as part of planned audits and providing this information to ISB. In addition to this compliance audits as already operational in line with any data protection incident/breach and in line with ongoing ISB work plans (i.e audit of CCTV devices, PCI usage) Implementation Date: September 2014 Owner: OM, Improvement & Information & OM, Audit & Risk Manager	
A19. Set challenging but realistic and achievable incremental compliance targets for training completion and reduction of data security breaches.	Accept – The Council's training compliance target with e-learning completion is 100% as set out within quarterly Information Security Performance Reports. An incremental compliance	

	target for the periods July, August, September of 90%, 95% and 100% will be set following approval by ISF on 17th June 2014, and monthly reports provided to each IAO. Targets for the reduction of data security breaches are already in place, and were in place and operational prior to the ICO Audit. Implementation Date: Immediate Owner: Information Governance Manager	
Training and Awareness		
B3. Ensure the Training Strategy for 2014-2016 is finalised and signed-off as soon as possible.	Accept – A draft Information Governance Training Strategy 2014-2018 is currently in consultation phase. Intended for to be finalised and operational by September 2014. Implementation Date: September 2014 Owner: OM, Improvement & Information & Information	

	Governance Manager	
B7. Ensure robust compliance monitoring of DP training to ensure the deadline of December 2014 is met. If necessary, prioritise training completion for new starters to ensure 'need to know' modules are completed as soon as possible after starting.	Accept – As outlined in a.19, the Council will continue to monitor training compliance and introduce incremental compliance targets. As part of this monitor modules of higher priority in terms of relaying significant Council Policy or statutory information will be prioritised to ensure compliance by December 2014. Implementation Date: Immediate Owner: Information Governance Manager	
B8. The Council should find a means of providing good quality data protection training to non - computer users. Providing reading material by itself is not sufficient to ensure that staff have an understanding of their obligations to comply with the	Reject	

Council's data Protection related policies and procedures. Consider supplementing the reading material with a classroom session and including a test element to ensure staff understanding.		
B9. Ensure that all staff with access to personal data, including non computer users, receive data protection related training before being given access to IT systems and/or manual documents containing personal information.	Partially Accept – The Council will investigate options as per b.9 to introduce a e-learning module covering the Council's core IG and Security policies prior to creation of an email account being set up. Implementation Date: October 2014 Owner: ICT Security & Compliance Manager & Information Governance Manager	
B10. Ensure all new starters complete all DP e-learning modules within a reasonable timescale of starting work.	Partially Accept – The Information Governance Training Strategy 2012-14 sets out employees requirements to complete e-learning training modules in	

	line with the Council's roll out of modules. The Council will investigate options as per b.9 to introduce an e-learning module covering the Council's core IG and Security policies prior to creation of an email account being set up. New starters including non computer users are required to attend Corporate Induction and a slot on this will be conducted by the OM Improvement & Information or IGM detailing the Council's IG responsibilities. Implementation Date: October 2014 Owner: OM Improvement & Information, Information Governance Manager & ICT Security & Compliance Manager	
B11. Develop mandatory data protection refresher training for all staff that can be monitored for take-up. The current training approach could	Accept – The Council will be implementing an Information Governance Training Strategy 2014-18 which will set out how refresher training will be	

be adapted for this purpose, for example, an e-learning module could be released periodically to remind staff of their obligations under the Data Protection Act.	provided. This Strategy will be operational from September 2014. Implementation Date: September 2014 Owner: OM Improvement & Information & Information Governance Manager	
B15. The Council should define a challenging but realistic target for training completion rates across all service areas, and state this within the reports to the ISF and ISB, so that reporting is measured against the target.	Accept – Training completion rates is already provided to ISB as part of quarterly performance reports. These reports will be altered to reflect new incremental completion target rates as set out in a.19 Implementation Date: Immediate Owner: Information Governance Manager	
Security of Personal Data		
C4. The IT Security Officer (ITSO) should be working towards a CESG certified professional certificate of competence. (see Local Public Services	Accept – This will be reviewed in line with process of directorate delivery planning and availability of budgets. ICT Service Manager has a Masters Degree in this area	

Data Handling Guidelines, v2 – Aug 2012).	of work. Implementation Date: January-March 2015 Owner: ICT Service Manager	
C11. Ensure the ISP is made available, in a suitable format, to staff and contractors who do not have access to a computer. The council should be able to provide a record that this has been done.	Accept – This will be reviewed as set out in A4. Implementation Date: October 2014 Owner: ICT Service Manager	
C12. Consider developing a policy review process that will ensure ISB has oversight of all existing IG and IT policy reviews and will be involved in new policy development at an early stage. All IG policies should be logged by the I&IM Team and be subject to periodic review.	Accept – A Policy Review Process will be developed to ensure all IG and IT policies are annually reviewed by ISB Implementation Date: August 2014 Owner: Information Governance Manager	
C13. Ensure all existing IG and IT policies are reviewed to ensure they are up-to-	Accept – As per action set out in c12 Implementation Date:	

date, suitable and accurate. Each policy must have an appropriate cover sheet showing version control, author, owner and who has approved and signed the policy off.	August 2014 Owner: ICT Service Manager, OM, Improvement & Information & Information Governance Manager	
C26. Ensure all existing IT contracts held with third parties who have access to Council held personal data are reviewed to ensure they contain appropriate data protection and confidentiality clauses. These should be periodically reviewed to ensure clauses are still relevant and up-to-date.	Accept – Changes to be made to the Council's Contract Award Procurement process to highlight need to complete PIA's and ensure appropriate protocols or agreements are in place with third parties processing data. Existing contracts will be reviewed in line with review periods of such contracts and appropriate agreements put in place if not already identified. IAO will be tasked with reviewing contracts with third parties as part of Service Area Risk Register return Implementation Date: Immediate and ongoing Owner: Information Security	

	Board Members (IAO's), OM Improvement & Information & ICT Service Manager	
C27. Conduct a risk assessment of the security arrangements at the secondary staff entrance to ensure building security is not comprised by inappropriate tailgating.	Accept – Risk Assessment to be conducted by the Facilities Management Team, alongside IG & IT colleagues. Implementation Date: August 2014 Owner: OM, Facilities Management	
C28. Ensure Facilities management are provided with a weekly HR leavers list to ensure access cards that have not been returned can be deactivated as soon as possible.	Accept – The Council will set up a group consisting of IG, ICT, HR and Internal Audit, to investigate and implement an effective starters, leavers and movers list which for services requiring such information. Implementation Date: October 2014 Owner: OM, Improvement & Information, ICT Service Manager, Corporate Chief HR Officer	
C31. Ensure the new	Accept –	

confidential waste contract contains a more secure method of storing waste than open bags, for example locked containers.	New contract due to go live July 2014. This will replace current system of confidential waste collection in core buildings and replace with lockable bins. Implementation Date: July 2014 Owner: OM, Facilities Management & OM, Improvement & Information	
C34. Consider developing an official 'clear desk' policy to ensure staff are clear about their responsibility for securing personal data when they vacate their desk.	Partially Accept – The Council has adopted and provided staff with guidance on keeping their workplace clear. This has also been made available through specific e-learning training. The Council will consider developing local policies in line with office accommodation moves. Implementation Date: October 2014 Owner: OM, Improvement & Information	
C35. Review storage of keys for units containing personal	Accept – The Council will be setting each service IAO an action	

data and assess if digital key safes will provide a more secure access to storage solution.	to review storage of keys and safes within their services and introduce formal guidance for all staff Implementation Date: August 2014 Owner: Information Security Board	
C39. : Develop and implement a procedure to ensure HR provide regular staff lists of movers and leavers to both the IT service desk and the CareFirst and DigiGov system administration teams to ensure staff can be cross-referenced against Active Directory, CareFirst and DigiGov applications. Spot checks should be performed to ensure the procedure is working satisfactorily.	Accept – The Council will set up a group consisting of IG, ICT, HR and Internal Audit, to investigate and implement an effective starters, leavers and movers list which for services requiring such information. Implementation Date: October 2014 Owner: OM, Improvement & Information, ICT Service Manager, Corporate Chief HR Officer	
C40. See C39.	As recommendation 39	
C43. Ensure all VPN access to CareFirst is authorised through the ICT service desk to	Accept – Access is currently logged but the Council will review the authorisation processes	

enable an access log to be recorded and comply with the Council's ICT Security policy.	Implementation Date: October 2014 Owner: ICT Service Manager	
C44. Staff ability to save data to a CD/DVD writer is a risk that requires assessment and mitigation. A review of staff who have write access to CD/DVD drives is advisable to ensure this function is still required by those staff.	Partially Accept – The Council do not allow by default use of CD/DVD. Officers would have to specifically request and outline why this wish for such facilities. ICT can and do challenge this, and such devices are not authorised without Operational Manager approval. It is the responsibility of the Service Operational Manager to ensure that pc's with such devices are retained within the service area for the operational reason they were supplied and to review this use Implementation Date: Immediate Owner: ICT Service Manager	
C45. Vulnerabilities discovered in Windows XP will not be addressed by new	Partially Accept – An ongoing programme to upgrade all pc's onto Windows 7 is already	

Microsoft security updates. Ensure that any security issues resulting from the Council running PCs using this software have been risk assessed and mitigated.	operational Implementation Date: Immediate Owner: ICT Service Manager	
C46. Ensure the security features of AppLocker are in force on all council desktops, especially ones which have not been upgraded to Windows 7.	Partially Accept - AppLocker is only available on Windows 7 and in line with c45 the Council has an operational programme in place at present to upgrade all pc's onto Windows 7 Implementation Date: Immediate Owner: ICT Service Manager	
C48. A requirement of the PSN CoCo is to ensure Protective Markings are used on all documents being sent through PSN. Investigate measures to ensure adherence to this requirement.	Accept – A business case will be submitted to the SIRO investigating options for ensuring the Council complies with the Government Protective Marking Scheme, and a Protective Marking Policy to be developed and approved by Cabinet	

	Implementation Date: August 2014 Owner: Information Governance Manager & ICT Security & Compliance Manager	
C49. Review the policy of allowing staff to keep email indefinitely to ensure that staff are not breaching the Council's records management retention and disposal schedules or Principle 5 of the DPA.	Partially Accept – The retention of email depends upon its content and is therefore not possible to set against specific retention periods. However this will be reviewed in line with the deployment of the EDRMS as emails of business value will be expected to be stored within the EDRMS and matched against content types, therefore ensuring they are retained for lawful purposes. As part of each service deployment onto the EDRMS reviews will be conducted into the storage of emails outside of the EDRMS to ensure the Council complies with Principle 5 of the Data Protection Act Implementation Date: ongoing in line with 3 ½	

	year Implementation Programme of the EDRMS Owner: OM, Improvement & Information & Information Governance Manager	
C51. Ensure there are strictly enforced guidelines and procedures in place to ensure staff are not using webmail to download and save personal data onto home computers.	Accept – Webmail facility to be switched off in line with PSN requirements Implementation Date: October 2014 Owner: ICT Service Manager	
C52. Investigate why the password complexity rule is not enforced in CareFirst and remedy this if it is technically possible. The Care First application should adhere to the password policy requirements stated in the Council's ISP.	Accept – Password control within CareFirst to be reviewed Implementation Date: September 2014 Owner: OM, Assessment & Care Management & ICT Security & Compliance Manager	
C67. Ensure the I&IM Team has an overview of all current and future web applications and cloud computing storage where personal	Accept – This will be addressed through process changes identified within c.26 Implementation Date:	

data is involved.	Immediate and ongoing Owner: OM, Improvement & Information & Information Governance Manager	

I can confirm that this management response is a true representation of the current situation regarding progress made against our Action Plan outlined in the ICO Data Protection Audit Report dated 16 June 2014.

Signature…….

Print name……..

Position……..

Organisation……

Date……..

Item 7.1

Information Governance in the City of Cardiff Council

City of Cardiff Council

Audit Committee September 2014

Legislative background

- Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Human Rights Act 2010
- Privacy and Electronic Communications Regulations 2003
- Protection of Freedoms Act 2012
- Local Government (Wales) Measure 2009

Key elements

- Legislative framework
- Information requests
- Information security
- Information as an asset
- Information sharing

Information Requests

- Freedom of Information
- Subject Access Requests and requests under the non disclosure provisions of the Data Protection Act

Key Risks

- Enforcement action by Information Commissioner
- Financial penalties of up to £500k issued by Information Commissioner (Data Protection Act)
- Damage to the Council's reputation

Information Security

- Management of information in line with Data Protection requirements
- Covers both paper and electronic information
- Records Management and classification

<u>Key Risks</u>

- Financial penalties of up to £500k issued by the Information Commission (DPA)
- Damage to the Council's reputation

Information as an asset

- Proactive management of information
- Maximise the use of information held
- Working towards evidence based decision making

Key Risks

- Culture of the organisation and ability to change
- Staff capacity to deliver this significant agenda

Information sharing

- Signed up to the Wales Accord for the Sharing of Personal Information (WASPI)
- Ensure that where we share or need others to process data we do so legally and appropriately

<u>Key Risks</u>

- Enforcement action by Information Commissioner
- Financial penalties of up to £500k issued by Information Commissioner (DPA)
- Damage to the Council's reputation

What are the external views?

- The ICO Consensual Audit in April 2014 assessed the Council has having a reasonable level of assurance but with opportunities to improve
- WAO recognition that there has been a significant improvement around key aspects of the Information Management Agenda

What do we need to improve?

- Governance of information as an asset
- Update relevant IT policies
- Roll out refresher training for staff across the Council
- The arrangements for dealing with confidential waste
- Increase the range of pre-published information
- Maximise the use of an EDRMS

Information Governance in the City of Cardiff Council

City of Cardiff Council

Audit Committee December 2014

Legislative background

- Data Protection Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Human Rights Act 2010
- Privacy and Electronic Communications Regulations 2003
- Protection of Freedoms Act 2012
- Local Government (Wales) Measure 2009

Key elements

- Legislative framework
- Information requests
- Information security
- Information as an asset
- Information sharing

Information Requests

- Freedom of Information
- Subject Access Requests and requests under the non disclosure provisions of the Data Protection Act

Key Risks

- Enforcement action by Information Commissioner
- Financial penalties of up to £500k issued by Information Commissioner (Data Protection Act)
- Damage to the Council's reputation

Information Security

- Management of information in line with Data Protection requirements
- Covers both paper and electronic information
- Records Management and classification

Key Risks

- Financial penalties of up to £500k issued by the Information Commission (DPA)
- Damage to the Council's reputation

Information as an asset

- Proactive management of information
- Maximise the use of information held
- Working towards evidence based decision making

Key Risks

- Culture of the organisation and ability to change
- Staff capacity to deliver this significant agenda

Information sharing

- Signed up to the Wales Accord for the Sharing of Personal Information (WASPI)
- Ensure that where we share or need others to process data we do so legally and appropriately

Key Risks

- Enforcement action by Information Commissioner
- Financial penalties of up to £500k issued by Information Commissioner (DPA)
- Damage to the Council's reputation

What are the external views?

- The ICO Consensual Audit in April 2014 assessed the Council has having a reasonable level of assurance but with opportunities to improve
- WAO recognition that there has been a significant improvement around key aspects of the Information Management Agenda

What do we need to improve?

- Governance of information as an asset
- Update relevant IT policies
- Roll out refresher training for staff across the Council
- Increase the range of pre-published information
- Maximise the use of an EDRMS

Progress against ICO findings

Of the 36 Recommendations:

- 23 are completed
- 12 are partially completed
- 1 is not yet started

This recommendation is in respect of a review of staff who have ‘write’ access to CD/DVD drives. This work will be undertaken by ICT in January 2015

Progress against ICO findings

Data Protection Governance (9)

- 6 Completed
- 3 Partially Completed

Training & Awareness (7)

- 7 Completed

Security of Personal Data (20)

- 10 Completed
- 9 Partially Completed
- 1 Not Yet Started