Brent	**Audit Committee** 5 January 2016 **Report from the Director of Policy Partnerships and Performance**
For Action	Wards affected: None

Information Commissioner's Office Audit

1.0 Summary

1.1 This report outlines the position with the Information Commissioner's Office (ICO) data protection audit.

1.2 It outlines the Council's action plan to address the findings from the audit.

1.3 It also list the outcome of similar audits conducted at other Local Authorities recently.

2.0 Recommendations

The Committee is asked to:

2.1 Review the Executive Summary from the ICO audit.

2.2 Endorse the Action Plan to address the audit recommendations.

2.5 To note that the Executive Summary of the ICO audit will be published on the ICO website.

3.0 Details

3.1 ICO Data Protection Audit

3.1.1 An invitation to undertake a data protection audit by the ICO was received dated 23 January 2015. The purpose of the audit is to provide the Information

Commissioner and the Council with an independent assurance of the extent to which the Council, within the scope of this agreed audit, is complying with the Data Protection Act 1998 (DPA). The assurance and recommendations are assessed against best practice.

3.1.2 The ICO's auditors came on site on 8th, 9th and 10th September 2015. They concentrated on three areas:

- Security of personal data
- Subject access requests
- Data sharing

3.1.3 On 2 November 2015, the council received the final version of the auditor's reports. One report contained an executive summary, which is publishable, and the second contained the detailed findings and a proposed action plan. The Council completed its responses to the recommendations, which were agreed by the ICO's Audit team.

3.1.4 The Audit provided an overall conclusion of Limited Assurance (Amber grading). This states there is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA.

3.1.5 The Audit provided a conclusion of Reasonable Assurance (Yellow) for Security of Personal Data, and Limited Assurance for Subject Access Requests and Data Sharing (Amber).

3.1.7 The associated action plan has been formalised by the ICO and included under Attachment A. The implementation of the plan is monitored and overseen by the Corporate Information Governance Group. The target is to complete all the actions by May 2016.

3.1.8 The executive report identifies the main areas of improvement, and the most significant ones are:

- Improved technical controls for portable memory devices. This equates to blocking these devices from the network
- Implementing annual mandatory refresher training for all staff and contractors. Currently, training is required every four years
- Increasing the target for complying with the SAR statutory timeframes to 95% sooner. Currently the target is 80% for 2015 and 95% for 2016.

3.1.9 The ICO will undertake a purely desk based follow up of the audit in the next 6-9 months. This will assess progress against recommendations shown in Attachment A and should include senior sign off at Chief Executive or Board member level. They will contact the council in approximately a month before the follow up exercise to formalise the arrangements for this.

3.1.10 Attachment B summarises the findings of other Local Authorities that have been audited recently.

4.0 Financial Implications

4.1 None.

5.0 Legal Implications

5.1 None.

6.0 Diversity Implications

6.1 None.

7.0 Staffing/Accommodation Implications (if appropriate)

7.1 None.

Background Papers

Information Commissioner's Audit – Executive Summary (LBoB - executive summary.pdf)

Contact Officers

Peter Gadsdon, Director, Policy Partnerships and Performance
Rajesh Seedher, Information Governance Manager

Attachment A – Detailed Findings and Action Plan

Area	Findings	Action	Target	Responsible
Security	A 2. LBBC should implement standard document and version control for all key information governance policies and procedures to provide staff with assurances that all policies are reviewed on an annual basis, that they are the most up to date versions and to provide a historical record of all changes that have been made during the lifecycle of the policy.	To review all key information governance policies and procedures to ensure they have consistent format and version control. CMT to agree statement that all key information governance policies and procedures to be reviewed annually	Dec-15	Information Governance Manager
Security	A 5. LBBC should ensure that all staff that are mandated to read and sign acceptance of the Access to Information Rulebook do so within a timely manner. They should also undertake measures to improve their corporate monitoring of policy acceptance and compliance, for example via the utilisation of 'CALMS' (training software) in respect of key information governance and security policies and guidance.	To incorporate this function with the upgrade to CALMS during January 2016	Mar-16	Information Governance Manager
Security	A 9. Document a procedure to ensure information security risk assessments take place on an appropriate and regular basis.	Revised change procedure	Dec-15	Head of Infrastructure and Delivery

Area	Findings	Action	Target	Responsible
Security	A17. Ensure provisions are in place to mitigate the risk in the event of the Information Governance Manager leaving or being absent long term from the organisation.	Information Governance Manager to train Information Governance team members to provide cover	Jan-16	Information Governance Manager
Security	A20. Carry out training needs analysis to provide assurances for level and consistency of knowledge for individuals undertaking the role of an IAO (Information Asset Owner).	IAO to complete a training needs analysis form and to follow up requirements via a classroom base training session	Mar-16	Information Governance Manager
Security	A24. Ensure all risk registers are updated when risks reach their target date.	Audit and investigation to document procedure to update risk before they reach their target date	Dec-15	Head of Audit and investigation
Security	A25. Ensure PIA's (Privacy Impact Assessments) are carried out for all new and changes in processes which involve personal data supplemented by a requirement of when to carry out a PIA documented in policy.	Update the change process to incorporate PIA being done when there is change involving personal data	Dec-15	Head of Infrastructure and Delivery
Security	A28. Develop a training needs matrix to identify and document appropriate information security training courses and enable those who require specialist information security training for their role to be identified.	To conduct a training need analysis to identify specialist training requirements using a training matrix. Then schedule a programme of training.	Apr-16	Information Governance Manager
Security	A30. Ensure all staff complete the mandatory four e-learning courses in a timely manner and that reports produced capture all employees. Report training completion rates to an appropriate group (eg the IGG) to provide	To implement automated reminders to staff in the new version of CALMS, and automated reporting to services. To ensure that training performance is part of the IGG agenda.	Mar-16	Information Governance Manager

Area	Findings	Action	Target	Responsible
	(Information Governance Group).			
Security	A31. Document the training follow up process in a formal procedure which includes targets for managers to adhere to, to ensure training is completed by their reports within a set timeframe where it has been identified that there is a gap in completion.	CMT to agree statement around training. To add training performance to the corporate statistics.	Feb-16	Information Governance Manager
Security	A32. The ICO would recommend that some form of general staff data protection and information security refresher training, or awareness campaign is delivered on an annual basis. Where this is not feasible or practicable, then the organisation should have a documented refresher training plan in place to document the rationale and make the agreed frequency clear.	To incorporate annual training in the new version of CALMS, which will refresh training after 12 months.	Mar-16	Information Governance Manager
Security	A36. Document procedure for regular review of IAR and implement review.	The IAR procedure will be updated to incorporate regular review. IAOs will be instructed to update the current IAR.	Jan-16	Information Governance Manager

Area	Findings	Action	Target	Responsible
Security	A37. Ensure all laptops are added to the asset register.	Asset register to be updated	Dec-15	Head of Infrastructure and Delivery
Security	A40. Implement some form of end point control to restrict the import or export of data or malware using media.	To block USB memory sticks	Jan-16	Head of Infrastructure and Delivery
Security	A44. Correct Mobile iron's "check in" system to ensure mobile devices security measures are updated as appropriate.	To ensure that a documented procedure is in place to ensure that mobile devices security measures are updated.	Dec-15	Head of Infrastructure and Delivery
Security	A48. Ensure targeted security checks of high risk areas such as the server room are carried out.	High risk areas to be identified an included in the daily security check	Dec-15	Head of Infrastructure and Delivery
Security	A71. Update Records Management Policy to document role of Information Asset Owners with regards to setting and reviewing retention and disposal dates.	Record Management Policy to be updated to document the role of the IAOs with regards to setting and reviewing retention and disposal dates.	Jan-16	Information Governance Manager
Security	A73. Review and where necessary update the Cryptography Policy.	The Cryptography policy to be included in the annual review of policies.	May-16	Information Governance Manager

Area	Findings	Action	Target	Responsible
Security	A86. Ensure all losses of mobile devices are reported so they can be investigated appropriately and any lessons learned.	Update IT procedures and the Access to Information rule book to instruct staff to report all losses of mobile devices to digital services	Dec-15	Head of Digital Service
Security	A90. Ensure briefings on new systems and processes are taking place at team meetings.	To incorporate briefings on new systems and processes in the change procedure/checklist	Dec-15	Head of Infrastructure and Delivery
Subject access requests	B 1. Ensure that job descriptions include specific subject access responsibilities.	JDs will be reviewed and where generic descriptions do not cover specific SAR responsibilities they will be modified.	Apr-16	HR Director
Subject access requests	B 3. a) LBBC should consider making the location of the data protection page more immediately obvious from the homepage, for example via a quick link on the homepage footer. b) LBBC should clarify the contact details section of the leaflet to provide appropriate context as to when to contact LBBC and when to contact the ICO.	To consider adding a quick link on the homepage footer and the leaflet will be modified to provide context as to when to contact LBBC and when to contact the ICO.	Feb-16	Information Governance Manager
Subject access requests	B 4. The Service leads should periodically discuss and provide feedback to the IGT to resolve common problems or promote areas of good practice, for example by providing a regular update to the IGT or meeting as a forum.	To arrange quarterly meeting to discuss any issues and feedback to information governance group.	Jan-16	Information Governance Manager

Area	Findings	Action	Target	Responsible
Subject access requests	B 8. LBBC should amend the DPP and the Access to Information Rule Book to include reference to the specific DPO email inbox in the context of the subject access sections. LBBC should also ensure that such policies do not refer to corporate or local guidance (explicitly or implicitly) which may have existed under the previous subject access handling process.	To amend the DPP and the Access to Information Rule Book to incorporate the DPO email inbox and to remove references to the previous subject access handling process.	Jan-16	Information Governance Manager
Subject access requests	B 9. LBBC should amend the DPP to remove the reference to information requests via email being invalid.	The DPP policy to be updated to allow for email requests.	Nov-15	Information Governance Manager
Subject access requests	B11. LBBC should amend the IGT guidance to incorporate the process in respect of subject access requests for open Social Care cases.	Guidance for IGT to be updated to include open cases	Nov-15	Information Governance Manager
Subject access requests	B13. LBBC should ensure that contracts specify data processor obligations with regard to subject access, principally the requirement to notify LBBC upon receipt of a request, who they need to notify at LBBC, how and within what timescale.	To implement changes to new or reviewed contracts	Mar-16	Legal Contract lawyer

Area	Findings	Action	Target	Responsible
Subject access requests	B17. LBBC should ensure that Infostore includes fields to denote which specific systems have been searched for the requested information, whether specific subject exemptions or redactions have been applied and whether there has been any quality assurance in respect of the response. This will improve oversight of subject access compliance as well as monitoring of the status of individual requests.	To update infostore to include the names of the systems searched, whether exemptions or redactions have been applied and whether quality assurance was carried out.	Dec-15	Information Governance Manager
Subject access requests	B19. LBBC should ensure that the CMT reports include the number and nature of subject access complaints.	To include data protection complaints on future CMT reports	Feb-16	Information Governance Manager
Subject access requests	B22. LBBC should ensure that they have a formally established plan to achieve a KPI of 90-95% in respect of subject access compliance within a reasonable timeframe, monitor performance against this target and include this KPI within monitoring reports.	To include the 90-95% target in the CMT report	Feb-16	Information Governance Manager
Subject access requests	B23. LBBC should ensure that they prioritise requests which are in danger of falling outside the statutory 40 calendar day period as failing to comply with this period constitutes a breach of the DPA.	To update the SAR monitoring process to prioritise requests that are in danger of failing to comply with the 40 calendar day period.	Jan-16	Information Governance Manager

Area	Findings	Action	Target	Responsible
Subject access requests	B25. LBBC should amend the content of the Data Protection e-learning to reflect the current process for handling subject access requests, in particular the requirement for all requests to be forwarded to the DPO mailbox and that it is LBBC's corporate policy not to levy a fee.	To update the data protection elearning course content to include the use of the DPO mailbox and to inform staff that LBBC do not apply a fee. This will be done as part of the new update of the CALMS system.	Mar-16	Information Governance Manager
Subject access requests	B26. LBBC should enforce the same high pass mark for completion of the Data Protection e-learning on a corporate basis.	To include pass mark ratings in the training performance reports to services, and discussion at the IGG meetings	Mar-16	Information Governance Manager
Subject access requests	B29. LBBC should ensure that all employees with core responsibilities for subject access requests receive specialised training and that relevant records of this are maintained.	To carry out a needs analysis and to provide specialist training to staff that deal with SARs.	Mar-16	Information Governance Manager
Subject access requests	B31. LBBC should provide a standard form of authority for third parties, perhaps within the template subject access form, to ensure that such is fit for purpose.	To amend the council's subject access request form to include a template for authority and a list of acceptable proof of identity.	Jan-16	Information Governance Manager
Subject access requests	B34. LBBC should amend the template correspondence to clarify that the requester should raise any complaint about the subject access request directly with them and progress the complaint with the ICO only if and when they are unable to resolve the matter with LBBC.	To amend the SAR templates to ensure that complaints should be raised initially and directly with the council first before raising matters with the ICO	Dec-15	Information Governance Manager

Area	Findings	Action	Target	Responsible
Subject access requests	B37. LBCC should ensure that where detailed redactions are proposed by Service leads, these are accompanied by the relevant rationale which is documented for the IGT.	To update the instructions to the providers of SAR data to include rationale for any proposed redactions and to document this in the SAR system.	Jan-16	Information Governance Manager
Subject access requests	B42. Outline purpose for processing, recipients to which data may be disclosed, exemptions applied for redactions where able to do so and the systems searched for requested information in all SAR responses to data subjects. Adjust any template responses as necessary.	To update the template for sending information to recipients to include the systems searched and also any exemptions that were applied if it is appropriate to do so.	Dec-15	Information Governance Manager
Data sharing	C 3. LBBC should amend the IGG terms of reference to include relevant document controls and outline the IGG chair, membership and responsibility for the oversight of all data sharing. The Council may wish to refer to the ICO's Data Sharing Code of Practice in this regard.	To update the IGG terms of reference in accordance with the ICO's Data Sharing Code of Practice	Feb-16	Information Governance Manager
Data sharing	C 5. LBBC should ensure that job descriptions in respect of individuals with key roles in systematic data sharing or one-off disclosures include specific corresponding responsibilities. The Council may wish to refer to the ICO's Data Sharing Code of Practice in this regard.	JDs will be reviewed and where generic descriptions do not cover specific data sharing responsibilities they will be modified.	Apr-16	HR Director

Area	Findings	Action	Target	Responsible
Data sharing	C 7 . LBBC should amend the content of the Data Protection e-learning to include basic guidance in respect of what systematic data sharing is and who should be consulted, and to highlight the Brent Information Sharing Code of Practice.	To update the elearning Data Protection course as part of the updated CALMS system to include basic guidance around data sharing and to highlight the Brent Information Sharing Code of Practice	Feb-16	Information Governance Manager
Data sharing	C 9. LBBC should amend the BIS COP to detail Service level responsibilities in respect of systematic data sharing.	To amend the BIS COP to detail Service level responsibilities in respect of systematic data sharing.	Jan-16	Information Governance Manager
Data sharing	C11. LBBC should amend the corporate induction checklist to specify key data sharing policies new starters must read.	To amend the corporate induction checklist to specify key data sharing policies new starters must read.	Mar-16	HR Director
Data sharing	C16. LBBC should ensure that all DSAs and Protocols explicitly cover fair processing, including relevant exemptions. The Council may wish to refer to the ICO's Data Sharing Code of Practice in this regard.	For the DSAs that LBBC are able to change, fair processing is to be included. To include this in the Brent Information Sharing Code of Practice.	Feb-16	Information Governance Manager
Data sharing	C17. LBBC should ensure that fair processing requirements are set out in corporate policies relevant to data sharing. The Council may wish to refer to the ICO's Data Sharing Code of Practice in this regard.	To review policies that are relevant to Information sharing to ensure fair processing requirements are set out.	Mar-16	Information Governance Manager
Data sharing	C19. LBBC should ensure that all DSAs (Data Sharing Agreements) which may involve the obtaining of consent contain template forms.	For the DSAs/Protocols that LBBC are able to change, consent template forms are to be included. To include this in the Brent Information Sharing Code of Practice	Feb-16	Information Governance Manager

Area	Findings	Action	Target	Responsible
Data sharing	C23. LBBC should underline the need to consider data minimisation within the PIA template.	To amend the PIA to include explicit statement to consider data minimisation	Dec-15	Information Governance Manager
Data sharing	C25. To be effective the PIA process must include consideration of all the relevant factors. LBBC should ensure that the PIA template documents the complete, accurate and consistent consideration of these factors. The Council may wish to refer to the ICO's Conducting Privacy Impact Assessment Code of Practice in this regard.	To update the PIA in accordance with the ICO's Conducting Privacy Impact Assessment Code of Practice	Dec-15	Information Governance Manager
Data sharing	C27. a) LBBC should amend the BIS COP (Code of Practice) to include a copy of the corporate data sharing template agreement. b) LBBC should raise awareness of and monitor use of the corporate data sharing template agreement.	To modify the BIS COP to include a copy of the corporate data sharing template agreement. To improve awareness and monitor use of the template by updating the Information Governance web page.	Feb-16	Information Governance Manager
Data sharing	C28. LBBC should ensure that all signatories to DSAs sign accompanying statements of compliance.	To write to the authors of the DSAs and request an amendment to contain a statement of compliance during the next review. To include a template statement on compliance in the Brent sharing template	Mar-16	Legal Contract Lawyer
Data sharing	C29. LBBC should ensure that all DSAs cite and implement a review cycle.	To write to the authors of the DSAs and request an amendment to contain a statement of compliance during the next review.	Mar-16	Legal Contract Lawyer

Area	Findings	Action	Target	Responsible
Data sharing	C31. LBBC should ensure that DSAs provide specific detail as to how data will be securely shared. The Council may wish to refer to the ICO's Data Sharing Code of Practice in this regard.	To write to the authors of the DSAs and request an amendment to contain a specifics of how data should be shared securely.	Mar-16	Legal Contract Lawyer
Data sharing	C32. Update MASH and WSIC DSAs to include organisational points of contact who have involvement in day to day sharing arrangements.	To write to the authors of the DSAs and request an amendment to contain organisational points of contact.	Mar-16	Legal Contract Lawyer
Data sharing	C34. LBBC should ensure that they complete outstanding entries in the Information Sharing Register and that those entries relate strictly to data sharing arrangements with other data controllers.	To update the Information Sharing Register to complete the outstanding entries	Mar-16	Information Governance Manager
Data sharing	C35. Carry out review of template agreement and ensure all DSA's conform to it.	To review known DSAs are compared against the template agreement and to write to the authors of the DSAs to suggest amendments if appropriate.	Mar-16	Legal Contract Lawyer
Data sharing	C36. LBBC should ensure that DSAs to which they are a party consider whether the shared data distinguishes between fact and opinion to help determine how shared data is viewed/used. The Council may wish to refer to the ICO's Data Sharing Code of Practice in this regard.	To review the DSAs and to write to the authors of the DSAs to suggest amendments if appropriate.	Mar-16	Legal Contract Lawyer
Data sharing	C37. LBBC should ensure that the DSAs to which they are a party require the source to inform recipients when shared data has been amended or updated.	To review the DSAs and to write to the authors of the DSAs to suggest amendments if appropriate.	Mar-16	Legal Contract Lawyer

Area	Findings	Action	Target	Responsible
Data sharing	C39. LBBC should ensure that the DSAs to which they are party contain specific provisions with regard to ensuring the quality of shared data.	To review the DSAs and to write to the authors of the DSAs to suggest amendments if appropriate.	Mar-16	Legal Contract Lawyer
Data sharing	C41. a) LBBC should ensure that the DSAs they are party to specifically prescribe that the recipients of shared data must destroy or return that data once the relevant purpose is served or any relevant retention period expires. b) LBBC should ensure that the DSAs and supporting procedural documentation specifically outline appropriate retention periods for shared data.	To review the DSAs and to write to the authors of the DSAs to suggest amendments if appropriate	Mar-16	Legal Contract lawyer
Data sharing	C43. LBBC should amend the DPP and the Brent Information Guide to include reference to forwarding requests to the DPO at the specific email inbox or postal address.	To modify the DPP to include reference to forwarding requests to the DPO at the specific email inbox or postal address.	Dec-15	Information Governance Manager
Data sharing	C44. LBBC should ensure that responsibility for responding to third party requests for disclosure continues to be undertaken by a relevant individual.	To ensure that following the restructure that the responsibility for responding to third party requires continues to be undertaken by a relevant individual.	Feb-16	Operational Director Strategic Commissioning
Data sharing	C46. LBBC should establish more in-depth verification procedures to confirm the identity of third party requesters to reduce the risk of disclosing personal data inappropriately.	To develop a verification procedure and update templates and website to include the verification procedures to confirm the identity of third party requestors.	Feb-16	Information Governance Manager

Area	Findings	Action	Target	Responsible
Data sharing	C48. a) LBBC should formalise the network of Service leads with responsibility for third party requests. b) LBBC should require Service leads to formally notify the Information Governance Team of all direct responses to requests and ensure that there is some form of approval of the response before it is issued at Service level.	To update the disclosure procedures to ensure that Service leads formally notify the IGT of all direct responses to request and that there is some form of approval at service level.	Mar-16	Information Governance Manager
Data sharing	C53. LBBC should specify the identity of the third party making the request for disclosure and include a field for exemptions within the Disclosure Log.	To create exemption and an ID verified fields in the disclosure log and also to update the disclosure procedure to include verification.	Feb-16	Information Governance Manager
Data sharing	C54. LBBC should ensure that they undertake periodic quality assurance assessments of one-off disclosures to satisfy themselves that they are handling such requests appropriately.	To include a quality assurance field in the disclosure log and to update the disclosure procedure to include assurance checks and criteria.	Feb-16	Information Governance Manager

Attachment B – Survey of Other Authorities Recently Audited

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
Islington - Feb 2015	Reasonable Assurance	There is a reasonable level of assurance that processes and procedures are in place and 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 two reasonable and one limited assurance assessments where controls could be enhanced to address the issues.	• Data Security Working Group (DSWG)in place • Mandatory IG training for all staff accessing network. • PSN accreditation, GCSx email system • Support for secure remote and agile working • There is a clear reporting mechanism for both data breaches and IT security incidents, with staff required to report all incidents (including 'near misses') to the IT Service Desk, who automatically escalate them to both the Data Security Manager and the Digital Services management team • All incidents are reported to both the DSWG and the Corporate Governance Group.	• IARs are not yet embedded and being used by IAOs to assess the risk to information held in their business areas • There are occasions when both new starters and locums are given access to the Adult Social Services system prior to receiving any training. • Call recording is not disabled when service users provide payment card details, which is a breach of the Payment Card Industry (PCI) • There is no centralised system for logging, processing and oversight of SARs,

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
Stoke-on-Trent -May 2015	Reasonable Assurance	There is a reasonable level of assurance that processes and procedures are in place and 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 two reasonable and one high assurance assessment where controls could be enhanced to address the issues	• Data protection awareness training has to be taken within six weeks of commencing employment at SoTCC • Where an individual is unable to book on a data protection awareness course within six weeks, Organisational Development will arrange to deliver the training one to one, desk side. • The data protection training is constantly being reviewed and refreshed based on feedback from delegates • The CRM system supplier is ISO 27001 accredited. All data held on the system is encrypted and in named data centres within the EEA. • The contracts with the system supplier include clauses relating to retention and disposal requirements • All agile workers are supplied with SoTCC laptops which includes Cisco IPSec	• Writable CD/DVD drives on desktop PCs are not locked down to prevent staff saving data to removable disks. • There is no working Information Asset Register (IAR) in place where information assets are identified, have owners assigned to them, are risk assessed and reviewed, and no information mapping exercises have been undertaken. • The Privacy Impact Assessment procedure has not been implemented

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
			VPN Client (which only authenticates known devices) and dual-factor authentication (utilising a physical token).	
Manchester City Council - May 2015	Limited Assurance	There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA. We have made one reasonable and two limited assurance assessments where controls could be enhanced to address the issues	• The Council have trained an established network of Information Asset Owners (IAOs) who have a good understanding of their data protection responsibilities • The Council have made a strong commitment to identifying staff who may have occasional access to personal data but do not have access to the DP e-learning on the corporate IT network. Training resources have been produced to enable managers to brief these staff at both formal classroom training and informally at team meetings. • Data protection and IT security incidents are	• The SIRO would have more effective oversight of cross-cutting information governance (IG) issues, and their mitigation, with the development of a corporate IG Risk Register, which should be regularly reviewed. • There is no individual officer with oversight of data protection training • Mandatory data protection e-learning has been rolled out to all staff with access to IT but the target date for completion of October 2014 was not met. There have been some resource issues around compiling accurate statistics due to the incompatibility of the reporting function of the

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
			reported via an online reporting tool. This automatically manages workflow and flags up incidents to Information Governance staff. • Staff are made aware of how to report incidents through the Information Security Incident Management procedure and all incidents are logged, remedial action identified and lessons learnt implemented. • A useful Subject Access Request (SAR) checklist is employed which divides the process into four distinct stages; subject access form and acknowledgement; locating and retrieving the data; exempting and redacting; and making the disclosure. This ensures a consistent approach to dealing with	module and the Council's Learning Management System. • New starters are required to complete the current mandatory data protection e-learning module. However, this module does not cover key areas of the Act, including the eight Data Protection principles and the right of Subject Access. • The Council should identify performance measures that reflect their SAR responsibilities and mitigate the risks that non-compliance with Principle 6 of the Data Protection Act may present to the authority. • Privacy Impact Assessment (PIA) guidance and templates are in the final stages of completion and the

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
			SARs.	obligation to carry out PIAs is about to be rolled out to commissioning and procurement teams. It is important these are embedded into all new projects involving personal data as soon as is practical.
Sefton Metropolitan Borough Council – Jan 2015	Limited Assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA. We have made three limited	• SMBC have recently created a governance structure with accountability and responsibility for data protection matters • A needs based training programme is now in place and will be rolled out across the Council. The training material was	• Data Protection/Information Governance policies and procedures are not adequate. • Although the IMG meet on a monthly basis, they do not have a formalised work plan or KPIs against which they can measure the progress and success of

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
		assessments relating to data protection governance, subject access requests and Freedom of Information governance and one reasonable assurance assessment relating to training and awareness where controls could be enhanced to address the issues.	produced by the Information Governance Trainer and DPO and informed by ICO guidance • The Council supply information in response to subject access requests (SARs) in an appropriate manner. • Software is used to redact information where required within responses to Freedom of Information requests.	their information governance initiatives. • Privacy Impact Assessments (PIAs) are not mandatory for any new system or process that involves the processing of personal data. • There is no specialised training provided for key information roles such as the SIRO, DPO, SAR and Freedom of Information (FOI) request handlers, to ensure they are capable of carrying out their job effectively. • There is a recognised lack of resource for responding to SARs. In addition to this, many of the processes that have been developed for responding to SARs have not been formalised within relevant policies and procedures, and relevant job descriptions do not

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
				reflect the responsibilities of staff. • Oversight of compliance with the Freedom of Information act 2000 is not adequate. FOI matters are not included as a standing item to be discussed at the IMG. • Clauses have not yet been included within contracts with partner organisations to ensure that they deal appropriately with FOI requests.
Cheshire West and Chester Council - December 2014	Limited Assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with the DPA. We have made three limited	• The importance of good information governance and security appears to have been recognised in the recent restructure • CWCC has been carrying out a gap analysis (in which this audit plays a part) following the restructure. It was encouraging for auditors to see that interviewees were	• The management of information risk is underdeveloped. There are no embedded Information Asset Owners reporting to the Senior Information Risk Owner • Information Risk and Information Asset Registers are incomplete. • There was clear evidence that some old incidents

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
		assurance assessments where controls could be enhanced to address the issues .	able to highlight deficiencies and existing action plans to deal with them, pre-empting many of the ICO's recommendations. • This awareness of current problems is informed by an active and engaged internal audit function, carrying out planned long-term audits and providing robust incident management follow-up • CWCC's privacy notices (provided on the website and by individual services) were generally thorough and informative.	were inappropriately scored and managed. • There was no current systematic reporting of performance indicators to enable monitoring of information governance • The security controls for some physical records and equipment disposal needed improvement, leading to a risk that information could be lost or stolen from storage areas.
London Borough of Tower Hamlets - Dec 2014	Limited Assurance	There is a limited level of assurance that processes and procedures are in place and delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the	• There is a management structure in place to coordinate and support Information Governance (IG) across the Council. • The Council has appropriate fair processing notices in place and	• Further development of the Information Asset Register is required, to include manual records, and be linked to the Council's retention schedules. • Records management function could be improved

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
		risk of non-compliance with the DPA. We have made one reasonable assurance assessment relating to security of personal data and two limited assurance assessments relating to records management and requests for personal data where controls could be enhanced.	provides an accessible booklet 'Your Records and You', which clearly explains how it obtains, holds, uses and discloses personal data. • The Council is compliant with the Public Service Network's (PSN) Code of Connection requirements, which allows it to connect to the secure GCSX network. They also adhere to ITIL for IT service management and have a framework for information security which includes other recognised standards including ISO 27001, the NHS' self-assessment IG toolkit and PCI DSS compliance.	by identifying performance measures that reflect their records management responsibilities and ascertain the risks that non-compliance • Performance measures and risks which have been identified should be documented and regularly reported to the Information Governance Group. • The Council should make greater use of their Internal Audit function to independently review the effectiveness of policies and procedures concerning IG, data protection, IT security and records management. • It is recognised that arrangements around starters / movers / leavers are in place but may benefit from being further enhanced.

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
				• A single Council-wide process for collection, storage and disposal of confidential waste should be introduced which will help provide assurance that waste is being managed securely. The Council should review the type of containers being used in offices to store confidential waste before disposal and the security of areas holding bulk confidential waste before collection by the contractors.
London Borough of Barnet - October 2014	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	• Security incidents are reported to the Information Management Team (IMT) and staff are made aware of how to do this via the Security Incident Management Policy. The IMT log and investigate incidents, identifying remedial action and lessons learned to	• Some security issues were identified during the audit and these should be addressed as soon as possible. These included some Council Offices potentially being accessible to non-staff members; confidential waste being stored in an unlocked post room and non council

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
		the DPA. We have made two reasonable assurance assessments in respect of requests for personal data and data sharing and one limited assurance assessment in respect of records management where controls could be enhanced to address the issues	ensure the incident does not recur. • The i-Casework case management system provides a detailed audit trail of how subject access requests have been handled. • Assigning "link officer" (LOs) responsibilities to members of staff at departmental level has been effective in enabling the Council to meet its subject access duties under the Data Protection Act. • A review of fair processing information given to data subjects has been undertaken and as a result, the standard fair processing notice has been improved and must be included on all data collection forms. • The process for information sharing with partner agencies is standardised via the Tier 1 and Tier 2 Information Sharing Protocols. Tier 1 sets out common rules to be followed by partners when sharing data and Tier 2	staff members being allowed to find their own way to meetings and events unescorted. • Information Asset Registers and associated Information Asset Owners are not yet in place • The Council should establish a register detailing the types of information held, how the information is used and transferred and who is able to access it. • Information assets should be assigned owners who should carry out regular risk assessments feeding the results to IMT and the SIRO as appropriate. • The retention schedule is not applied in a regular and systematic way to electronic and manual records. • The Council receive a number of section 29 requests for third party information, particularly within the corporate anti-fraud

Overall Conclusion				
Organisation	**Assurance Level**	**Summary**	**Areas of good practice**	**Areas for Improvement**
			outlines how data will be shared including the method of transfer, security, disposal and SAR response arrangements. Information Sharing Agreements are logged and are reviewed every 12 months to ensure they remain fit for purpose.	(CAF) team. It does not take sufficient steps to verify the identity of requesters and to ensure the requirements for disclosure of information under section 29 have been met. In addition to this, there is no consistent quality assurance or senior oversight of responses to section 29 requests. • Although work has been carried out to encourage use of PIAs, they are not mandatory.