Leeds City Council

Data protection audit report

Information Commissioner's Office

Auditors:	Christine Eckersley (Audit Team Manager) Chris Littler (Engagement Lead Auditor) Arleen O’Neill (Lead Auditor)
Data controller contacts:	Andrew Nutting (Executive Officer – Information Governance Department)
Distribution:	James Rogers (SIRO)
Date issued:	29 November 2013

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Leeds City Council.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

Contents

1. Background

1.1 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.

1.2 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.

1.3 Leeds City Council were the subject of ICO enforcement action in 2012 with both an Undertaking and a Civil Monetary Penalty issued for separate data protection breaches.

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

1.5 An introductory meeting was held on 25 June 2013 with representatives of Leeds City Council to identify and discuss the scope of the audit and after that through email and telephone correspondence to agree the schedule of interviews.

2. Scope of the audit

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

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

b. 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

3.1 The purpose of the audit is to provide the Information Commissioner and Leeds City Council with an independent assurance of the extent to which Leeds City Council within the scope of this agreed audit is complying with the DPA.

3.2 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 delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with the Data Protection Act. We have made two reasonable assurance assessments where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' section 7 of this report.

4. Summary of audit findings

4.1 Areas of good practice

- The Council have a robust management structure in place to coordinate Information Governance (IG) across the Council. A trained Senior Information Risk Officer is in post and there is an established Information Governance Management Board (IGMB) to provide an oversight of IG policies and procedures. Four sub-boards, with information assurance as part of their remit, report into the IGMB.

- 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. An annual breach report is provided to the SIRO.

- The Council is compliant with CESG's Code of Connection requirements, which allows them to connect to the GCSx network. They also align their IT infrastructure to comply with other recognised standards including ISO 27001 information security requirements and the NHS' self-assessment IG toolkit.

- The Council has an appropriate fair processing notice (FPN) in use within both children's and adults social services which clearly explains how it obtains, holds, uses and discloses personal data. A generic FPN is available on the Council's website and it is reviewing all data collection forms to ensure they contain a consistent FPN.

4.2 Areas for improvement

- Information Asset Owners (IAOs) are not systematically assessing risk to information 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.

- The off-site storage of manual records, including transport and retrieval, is well managed with a clear audit trail. However, there is no standardised procedure for ensuring social work case files, taken from individual offices on an ad-hoc basis, are recorded and monitored.

- Implementing a single Council-wide process for storage and disposal of confidential waste will help to provide assurance that waste is being managed securely. This should include a review of the type of office shredders being used to ensure they shred to required standards.

- The introduction of robust Privacy Impact Assessments and embedding them into the Council's project development and system design processes will help provide assurance that personal data risks are being assessed when new systems processing personal data are developed and implemented.

5. Audit approach

5.1 The audit was conducted following the Information Commissioner’s data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

5.2 The audit field work was undertaken at Leeds Civic Hall, Westgate Building, Apex Way, Merrion House, Hough Top Court, Westland Road, Killingbeck Court and Morley Town Hall between 1 – 3 October 2013.

6. Audit grading

6.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the following definitions.

Colour code	Internal audit opinion	Recommendation priority	Definitions
🟩	High assurance	Minor points only are likely to be raised	There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non compliance with the DPA.
🟨	Reasonable assurance	Low priority	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.
🟧	Limited assurance	Medium priority	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.
🟥	Very limited assurance	High priority	There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

7. Detailed findings and action plan

7.1 Scope: Records management. 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.

Risk: In the absence of appropriate records management processes, there is a risk that records may not be processed in compliance with the DPA resulting in regulatory action by the ICO, reputational damage to the data controller and/or damage and distress to individuals.

a1. The Senior Information Risk Officer (SIRO), who is the Assistant Chief Executive, has overall responsibility for records management within the Council. The Council has an Information Governance Management Board (IGMB), chaired by the Chief Officer, who has historically had responsibility for the Information Governance (IG) function. IGMB meets bi-monthly and regular items for discussion include legacy records, IG training, Information Asset Registers (IAR) and Incident Reporting.

a2. Day to day responsibility for the development and implementation of the records management function has been assigned to the Executive Officer of the IG team.

a3. The IG Executive Officer has a direct link to the SIRO with monthly meetings taking place in addition to the IGMB.

a4. The Council has four sub-groups which report into IGMB, including the Information Assurance Group and the Records Managers Group. Each group has defined Terms of Reference (TOR) and all meetings are minuted to show agreed actions and outcomes.

a5. The IG Executive Officer is supported by eight members of staff. In addition to this each Directorate has a Records Manager and an Information Compliance Officer (InCO), who have direct links to the IG team, to ensure that records are appropriately managed throughout the Council.

a6. Information Asset Owners (IAOs) are appointed at head of service level. Auditors were informed that the IAR is currently under review, and once completed IAO training will be rolled out.

Recommendation: Ensure IAOs are trained in line with proposed plans. Further advice on IAO training is available from The National Archives.

Management response: Accept.
A working group has been put together who are undertaking the information asset register project. This includes updating the register, developing an

improved technical solution for holding and updating information, identifying asset owners and providing relevant training, and developing procedures for appropriate reporting and management of information risk.

Implementation date: 01 October 2014

Responsibility: Information Governance Manager, Corporate Information Governance Team.

a7. The Council's Records Management policy has been endorsed by senior management and clearly sets out requirements for the records management function. The policy covers manual and electronic records, and includes details about security, storage, indexing, retention and disposal.

a8. The IG team is responsible for reviewing the policy with the next review scheduled for July 2014. There is a clear log showing the reviews carried out and that the policy is subject to version control.

a9. The policy is supported by the guidance available on the Council's intranet, and all staff interviewed knew where to find the policy and supporting guidance. Important updates are flagged to staff via the intranet or monthly IG newsletters.

a10. The Records Management policy sets out the training required to be undertaken by staff in relation to records management. The Council's IG team are responsible for producing records management training materials. However, the team does not currently have a permanent training resource with the current IG trainer being on a temporary contract.

Recommendation: It would be advisable to have a permanent resource within the IG Team to ensure that this essential training is developed, maintained and delivered over the long term.

Management response: Accept.
The council will ensure that the review of Information Management & Technology takes account of the need to provide mainstream IG training across the organisation (initial discussion on-going as part of budget planning process)

Implementation date: 01 May 2014

Responsibility: Head of Intelligence and Performance.

a11. It was reported that a number of the IG team do not have professionally recognised IG qualifications.

Recommendation: Members of the IG team should be suitably qualified to enable them to carry out their role effectively. It would therefore be advisable for the Council to provide relevant professional training.

Management response: Accept.
Funding for the corporate IG team is being considered as part of determining the budget for the

2014-15 financial year. Precise qualifications required to be determined in further discussion with the ICO.

Implementation date: 01 May 2014.

Responsibility: Head of Intelligence and Performance

a12. In addition, the IT Security Officer (ITSO) does not hold, nor is working towards, a CESG certified professional certificate of competence in line with the Local Public Services Data Handling Guidelines.

Recommendation: To comply with the Local Public Services Data Handling Guidelines, the Council should provide suitable CESG training for the ITSO.

Management response: Accept.
The council will provide suitable CESG training for theIT Security Officer.

Implementation date: 01 December 2014.

Responsibility: Chief ICT Officer

a13. The Council does not have specific Records Management training; it is included as a sub-section, which aligns to the RM Policy requirements, within a general IG training package. Because this training is relatively new, IG refresher training is not yet embedded, although there will be a requirement to complete every two years.

Recommendation: The Council should ensure regular IG refresher training is mandated and monitored to ensure staff knowledge is kept up to date and relevant.

Management response: Accept.
Staff who completed the Information Governance training in 2011/12 will receive a reminder to complete an updated version in April 2014. For PC users, completion will be recorded automatically on the Council's training system, and for non PC users the corporate Information Governance (IG) team will define and implement a procedure for logging their completion of the training. The content of training will be reviewed on a regular basis and an automated reminder will be issued to staff every two years to complete it again. Delivery of the IG training strategy includes more specific training needs analysis exercises and the development and delivery of more detailed training, for example Records Management training.

Implementation date: 01 June 2014

Responsibility: Senior Information Governance Officer (Training), Corporate Information Governance Team.

a14. Auditors were informed that training needs are identified by managers during one to one sessions, and that staff can request additional training via the Performance and Learning System (PALS). Requests for training sent via PALS must be authorised by a manager.

a15. The Council has specific trainers for the Electronic Social Care Records system (ESCR). Access is not granted to ESCR without training having been completed. There are however, rare occasions when a staff member may require urgent access to ESCR. In those cases a manager must authorise the access.

a16. The Council has an appropriate fair processing notice (FPN) in use within both children's and adult's social services. The FPN is a paper document which requires a signature and clearly explains how the Council obtains, holds, uses and discloses personal data. It also informs data subjects of their rights under the Data Protection Act (DPA).

a17. A generic FPN is available on the Council's website, providing details about personal data collected and reasons for its use. The FPN also provides information about the use of cookies on the website.

a18. The Council are currently reviewing all data collection forms to ensure they contain a consistent FPN. Forms will be refreshed to a consistent standard and a log kept.

a19. The majority of personal data is processed electronically using shared drives, which are access controlled, and electronic social care records. This has reduced the need for manual records to be held and used within social services to a minimum.

a20. There are occasions when staff within both the children's and adults social work teams are required to work on a manual file. These files are stored in locked team cupboards when not in use.

a21. The keys for the team cupboards are locked away in a drawer by a member of the administration team. The key for this drawer is then taken home. All members of the social work administration team have a key to the drawer. However if there are no members of the administration team in the office, social workers are unable to access the locked cupboards.

Recommendation: Provide digital key safes for use within social services teams to ensure that records are always accessible when required.

Management response: Partially accept.
Many social work offices already have effective mechanisms in place for accessing records out of core hours although it is recognised that consistency is required across social work areas. However, the Council does not regard the introduction of digital key safes as the most appropriate or cost effective option to address this issue. It intends to carry out a review of the current procedures in place across Adult Social Care and Children's Services with a policy to be then produced which addresses how

records are securely stored and accessed within offices.

Implementation date: 01 May 2014.

Responsibility: Jointly- Chief Officer, Partnership Development and Business (Children's Services), and Chief Officer, Learning Disabilities (Adult Social Care)

a22. Auditors noted that there are times when personal data is taken off site to enable social work staff to conduct home visits. The information taken on the visits is of a sensitive nature and is generally stored in social workers' bags; it is therefore not appropriately protected as the bags being used do not lock.

Recommendation: Provide a lockable storage solution for social workers taking manual personal records off site on client visits, such as lockable document holders, bags and/or car boot safes.

Management response: Partially accept.
The Council recognises the need for manual personal records to be transported in a secure manner. However, it does not consider that lockable transport means are a cost effective option or a proportionate response to preventing loss or theft. Instead the Council proposes to implement a policy which covers the circumstances in which records are to be taken out of social work offices and the most appropriate means, proportionate to the risk involved, by which they should be transported.

Implementation date: 01 March 2014.

Responsibility: Jointly- Chief Officer, Partnership Development and Business (Children's Services), and Chief Officer, Learning Disabilities (Adult Social Care)

a23. There is currently no standardised procedure in place for recording which records have been taken off-site. Children's social services record details of files taken out of the office in a log book which is monitored by the administration team, whereas the adults' social services team do not use any system of signing files out of the office.

Recommendation: Introduce a standard procedure for signing files out of the office and ensure the file returns are monitored.

Management response: Accept.
There is good practice in parts of the council, but it is recognised that this needs to be consistent across the organisation. The Corporate Records Manager will co-ordinate work to review current procedures and practice, develop and agree a corporate approach, and ensure these are in use within all relevant offices.

Implementation date: 01 September 2014.

Responsibility: Corporate Records Manager, Corporate Information Governanace team.

a24. Legacy paper records are archived off site at the West Yorkshire Archive Service (WYAS). There is a recording system in place which uses a combination of spreadsheets and bar-codes to enable the tracking and monitoring of those records. There are also regular box audits to ensure that boxes are tracked to the correct location within the archive.

a25. As well as using WYAS, the Council also has a contract in place with CINTAS for the storage of Council information. As part of this contract staff must sign a confidentiality agreement if they wish to visit the CINTAS site. This ensures that only approved individuals can access Council information at the CINTAS site.

a26. The Council has recently created a purpose built records management facility for the storage of its manual records. These were mainly social services records at the time of the audit.

a27. As part of the Council's RM facility, there is an associated RM database. The database is used by staff to recall boxes or files from the store and to request boxes and files are collected for storage at the RM facility. This enables real time tracking of council information. Quarterly reports are run to monitor which files are 'checked out' but there is no process in place to actively contact users who have not returned records to the RM facility.

Recommendation: Regularly monitor boxes and files which have been removed from the RM storage facility to ensure files are returned in a timely manner and enable the early identification of any missing records.

Management response: Accept
Current procedures will be reviewed with the records manager at the corporate facility, and revised in the short term as necessary. In the longer term the database that is used will be replaced by the e-Leeds programme. The requirement for enhanced monitoring will be taken in to account when the new system is developed.

Implementation date: 01 May 2014

Responsibility: Joint responsibility between Records Manager, Corporate Records Management Facility, and Programme Manager, E-Leeds programme.

a28. The Council has multiple sites, some purpose built and some public buildings. There were varying security controls within each building, ranging from swipe card access to door code access, although codes are not always changed on a regular basis. All buildings visited (except one) required the visitor's book to be signed and visitor passes were checked.

Recommendation: Ensure all visitors to office buildings containing sensitive personal data are recorded in a visitor's book and ensure codes for doors with pin code access are regularly changed and this is recorded.

Management response: Accept.
The council will introduce procedures to ensure all buildings have a book to record and monitor visitors. The procedure will include innstruction to change pin codes on a regular basis.

Implementation date: 01 September 2014.

Responsibility: Information Governance Manager, Corporate Information Governance team.

a29. The Council has a clear desk and clear screen policy. Spot checks for compliance with the policy are not routinely carried out in every department.

Recommendation: Implement a procedure for routine spot checking of compliance with the clear desk policy.

Management response: Accept.
An officer within the corporate IG team will be designated specific responsibility for co-ordinating monitoring of compliance with this and other IG policies. A procedure for spot checks for compliance with the clear desk and clear screen policy will be developed and implemented.

Implementation date: 01 September 2014.

Responsibility: Information Governance Manager, Corporate Information Governance team.

a30. Paperwork containing sensitive personal data is left in trays overnight in the Benefits Visitors' office as there are no lockable cupboards, although the office door is locked overnight.

Recommendation: Ensure all manual records containing personal data are locked away at the end of the day.

Management response: Accept.
With respect to the Benefits Visitors room, checks have been undertaken to ensure this room is locked daily and the service are providing a lockable cupboard to enable paperwork containing personal data to be locked away at the end of each day. Part of the procedures outlined in a28 will include instructions on when lockable storage should be provided and used within office space, and the council will assess the extent to which this is covered adequately in existing guidance. Monitoring of compliance will be included in broader work by the corporate IG team to monitor compliance with policy and procedure.

Implementation date: 01 September 2014. Note-lockable storage to be provided and in use within the Benefits visitors office by December 2013.

Responsibility: Assessment Unit Manager (Benefits) and Corporate IG team.

a31. Access to the Council's computer systems is controlled by role. The Council does not yet have a

Council wide electronic document management system (EDRMS). Staff are currently using a shared drive with files locked down by department and by role.

a32. In addition to the shared drive, social workers use the ESCR case management system. Access to the ESCR system is restricted until training has been completed. It is also restricted by team and sensitive files can be locked down (shielded) to specific staff members.

a33. ESCR has a limited in-built audit trail which cannot identify who has accessed a file or when it was accessed, but can identify changes to a file and by whom. To ensure access to ESCR is up-to-date a monthly report is produced which identifies any user who has not logged into the system for 6 weeks or more. Those identified have their access rights to ESCR revoked.

a34. It was reported that the children's social work team are subject to checks by the team manager and administration staff to ensure access rights to ESCR information remained role appropriate; auditors were unable to establish if this was standard practice throughout the Council.

a35. Auditors were informed that all staff with access to ESCR had to undertake and complete training before being granted access to the live system. It was also reported by all interviewees that passwords were subject to regular change.

a36. There is a system of peer checking for information being sent by post, and a safe haven fax procedure which staff interviewed were aware of.

a37. There are a variety of printers and multi-function devices (MFDs) in use at the Council. Some of the machines have 'follow-me' printing whereby a PIN number is required to retrieve print jobs and access features of the MFD.

Recommendation: Wherever available ensure that follow me printing is enabled. For devices which do not have follow me capabilities, introduce a system of spot checks to ensure information is not left on printers for any longer than necessary.

Management response: Accept.
Follow-me printing is currently the default for the majority of printers except where business units have requested an exception. The council will review these exceptions and re-instate follow-me printing where personal data is likely to be printed. Following this review, a system of spot checks and reporting will be introduced and implemented.

Implementation date: 01 June 2014.

Responsibility: Information Governance Manager, Corporate Information Governance team.

a38. There is a centrally managed function for the disposal of all redundant IT equipment. A log is kept of all equipment, which is tagged and stored in a secure area until collection. Equipment is then securely transported and destroyed to Government standards by an approved third party contractor. The process is monitored throughout its lifecycle and destruction certificates are provided at the end.

a39. It was reported that the Council has adopted but has not fully embedded the Government's Protective Marking Scheme (GPMS) as the scheme is currently under review. It intends to implement the Government's new protective marking scheme once it has been approved.

Recommendation: Ensure that the protective marking scheme is implemented as soon as is practicable.

Management response: Partially accept.
The Council has been waiting for the new classification from central Government, and has taken the decision to adopt the new classifications. We will be implementing the new protective marking scheme for all staff who use secure email. Testing of relevant software is planned for w/c 25th November and depending on the outcome of testing, a delivery plan will be developed for users of secure email.

Implementation date: 01 June 2014

Responsibility: Information Governance Manager, Corporate Information Governance team.

a40. The Council has an incident reporting procedure; interviews demonstrated that there is a good awareness of the reporting procedure among staff at all levels.

a41. Business Continuity and Disaster Recovery is in place for critical systems and testing is completed in line with an agreed schedule.

a42. The Council has a Records Retention and Disposal Policy which details how records will be created, stored and destroyed and there is a corporate retention and disposal schedule. However, interviews confirmed that five of the twenty-six sections of the schedule have yet to be signed off, and that the schedule has yet to be fully implemented for manual and electronic records across the Council.

Recommendation: Ensure that the retention schedule is finalised and implemented as soon as is practicable.

Management response: Accept.
The council will continue to define the work and resources required to implement the retention schedules. All schedules to be finalised and published, and delivery plans agreed by 01 June 2014.

Implementation date: 01 June 2014.

Responsibility: Corporate Records Manager, Corporate Information Governance team.

a43. The Council has a contract in place with a professional waste disposal company for the destruction of confidential waste for which a certificate of destruction is provided.

a44. It was reported that there are still some office areas where open bags are used for storing confidential waste, despite lockable containers being available if requested.

Recommendation: Ensure that offices which are using unsecured confidential waste bags are provided with the standard lockable containers which are part of the confidential waste contract.

Management response: Partially accept.
The council will review its policy regarding the use of confidential waste bags and assess whether a change in policy is required. Concurrently, an audit will be conducted to check where unsecured confidential waste bags are in use and then lockable containers will be provided where relevant, in accordance with policy.

Implementation date: 01 April 2014.

Responsibility: Joint responsibility between Corporate Information Governance team and Civic Enterprise Leeds (responsible for management of contract).

a45. Members of staff with responsibility for third party contracts carry out security visits to ensure compliance with the 7th Data Protection principle.

a46. Some areas, such as children's social services, have shredders instead of a confidential waste bin. Auditors inspected a number of shredders and ascertained that not all Council shredders are cross-cut shredders, including the one in children's social services. This is not a fully secure method of disposal, particularly in relation to sensitive personal data.

Recommendation: Carry out an audit of shredders and consider the introduction of cross-cut shredders for sensitive personal data, or the use of locked confidential waste bins with subsequent secure in-house or third party destruction.

Management response: Accept.
As per a44, a review of policy will be undertaken and information about shredder use will be collected as part of the audit outlined. LCC will consider the introduction of cross-cut shredders or confidential waste bins as appropriate.

Implementation date: 01 April 2014.

Responsibility: Joint responsibility between Corporate Information Governance team and Civic Enterprise Leeds (responsible for management of contract).

a47. Auditors were informed that ESCR does not have the functionality to implement automatic weeding. Staff informed auditors it can take up to an hour to manually remove a record from ESCR; removing a record from ESCR involves physically reviewing each case and deleting information field by field within each screen containing personal data. Therefore weeding of the ESCR system is time consuming and inefficient. However, the Council plans to introduce new social work casework systems over the coming year which contain the functionality to automatically weed records and should therefore rectify this problem.

Recommendation: Ensure ESCR files transferred to new casework systems are appropriately weeded in line with the Council's retention schedule.

Management response: Accept.
Prior to the implementation of both the Children's and Adult's casework systems a full review of the data to be migrated has been undertaken; including the data quality and retention of records. This will ensure that only those records which fall within the Council's retention schedule will be migrated onto the new systems. This work was concluded for Children's Services on 11/11/2013 when the new casework system went live. The review of data is still on-going in Adult Social Care, with a go-live date of 01/06/2013. Both Children's and Adult's new casework systems have the functionality for automatic review and deletions and are fully integrated with EDRM systems, enabling the review and deletion of attachments in line with the Council's retention schedule.

Implementation date: 01 June 2014.

Responsibility: Jointly- Chief Officer, Partnership Development and Business (Children's Services), and Chief Officer, Learning Disabilities (Adult Social Care)

a48. Service performance KPIs, including delivery timescales and volumes of records held, are being recorded, monitored and reported to the Senior Management Team by the Records Management facility. However, it was reported that these are not routinely reported to the IGMB.

Recommendation: Ensure that RM KPIs are routinely communicated to appropriate boards, including IGMB, from relevant sub groups.

Management response: Accept.
In order to address this recommendation, along with a49 and b4, the council will review current arrangements and establish suitable KPI's for all directorates, covering records management and all other aspects of the information governance framework. Following this, a system of monitoring, reporting, and communication of these KPIs will be implemented. In addition, the council will develop an assurance framework related to information risk and embedding policy. This will link with work on information asset management outlined under a6.
Implementation date: 31 December 2014

Responsibility: Head of Intelligence and Performance.

a49. Auditors were unable to establish whether Directorate level records managers or InCOs are made aware of, or report on, RM KPIs.

Recommendation: Establish suitable RM KPIs for all directorates and ensure these are appropriately reported within the IG structure.

Management response: Accept.
This will be addressed as part of work to meet recommendations a48 and b4.

Implementation date: 31 December 2014.

Responsibility: Head of Intelligence and Performance.

a50. Auditors were provided with evidence of Privacy Impact Assessments (PIAs) being carried out. These were based on ICO guidance.

a51. However, staff informed auditors that PIAs were not fully embedded as the Council is awaiting updated PIA guidance to be published by the ICO before rolling out PIAs across the Council.

Recommendation: Ensure that PIAs are embedded across the Council at the implementation stage of any projects involving the processing of personal data.

Management response: Accept.
Following the conclusion of the ICO consultation and any subsequent changes to the PIA process, the Council will embed PIA's in to the project manaegment framework.

Implementation date: 01 June 2014.

Responsibility: Information Governance Manager, Corporate Information Governance team.

7.2 Scope: 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.

Risk: Without robust controls to ensure that personal data records, both manual and electronic, are held securely in compliance with the DPA, there is a risk that they may be lost or used inappropriately, resulting in regulatory action against, and/or reputational damage to, the organisation, and damage and distress to individuals.

b1. There is an appropriate Information Governance Framework (IGF) in place for overseeing information security in the Council, including a current work plan of IG requirements and allocated IG roles and responsibilities, from the SIRO down. This is overseen by the IG team, who provide a corporate information governance function.

b2. IGMB leads on all IG related issues. It approves policy and provides guidance, standards and good practice in relation to IG. The Board comprises of senior staff from throughout the Council but its Terms of Reference (TOR) do not require the SIRO or the IT Security Officer (ITSO) to attend. In addition, the IGMB TORs provided for review are still marked-up as a draft.

b3. There is no formalised reporting to the IGMB of IG KPIs (Breaches / SARs / Records Management / IT security incidents etc.) from the four sub-boards that sit under it. However, there is a standing item on IGMB agenda for sub-group updates, which can either be verbal or in a brief report.

b4. Although the IGMB meeting minutes are published on the intranet there is no requirement for formal reporting of KPIs to the SIRO, the Risk and Performance Board or Internal Audit. However, IG issues can be raised through the IG team's Executive Officer at his regular monthly meetings with the SIRO.

Recommendation: Formalise a process for ensuring IG KPIs are reported to the IGMB from its sub-boards and these are recorded and formally reported back to both the SIRO and the Risk and Performance Board and/or Internal Audit.

Management response: Accept.
This will be addressed as part of work to meet recommendations a48 and a49.

Implementation date: 31 December 2014.

Responsibility: Head of Intelligence and Performance.

b5. There is an IKM / ICT Liaison Group which provides a formalised forum to maintain oversight of information security and links the IG team with the ICT team. The Group is alternately chaired by the Head of Intelligence and Performance and Head of ICT Strategy, Architecture and Commissioning. Members include the IG Executive Officer and the IG Manager. Meeting minutes reviewed demonstrate technical issues relating to information security are regularly discussed, with risks identified and actions and owners allocated as appropriate. Key issues from this forum are escalated to the IGMB.

b6. The ITSO is not a permanent member of this group, but does have regular, informal monthly meetings with the IG Manager.

Recommendation: Consider making the IT Security Officer a permanent member of the IKM /ICT Liaison Group so there is a clear reporting line to the SIRO, as recommended in the Local Public Service Data Handling Guidelines.

Management response: Accept.
The IT Security Officer will be added to the membership list of the IKM / ICT Liaison Group.

Implementation date: Immediate.

Responsibility: Head of Intelligence and Performance.

b7. The IGF acknowledges that the corporate ICT team play a major role in the delivery of information assurance throughout the Council. ICT endeavours to adhere to a number of recognised industry standards for information security, including ISO/IEC 27001, although this has not been extended to formal accreditation. A gap analysis has been undertaken on ITIL processes to benchmark existing processes against best practice standards.

b8. A key requirement for IT security is the necessity to comply with the GCSx Code of Connection, which entails annual self-assessment by the Council. The Council also complete the NHS IG toolkit and attained Level 2 in their 2012/13 assessment.

b9. The Council is currently developing a SIRO toolkit, based on the NHS IG toolkit, to enable IAOs to provide annual assurance to the SIRO on information security.

b10. The Principal Risk Management Officer is responsible for co-ordinating all strategic risk management arrangements. The strategic risk register comprises the most significant and cross-cutting corporate risks and includes Information Management. Corporate risks are reviewed quarterly by the Risk and Performance Board (which consists of senior managers from all directorates) and considered alongside other strategic management information by the Corporate Leadership Team (CLT) and elected members.

b11. New risks are proposed for inclusion in the corporate risk register through an escalation route and approved or rejected by CLT. These stem from risk registers kept at directorate, service and project level. Service areas with high risk, for example Adult's and Children's, include IG on their directorate risk registers. An additional corporate risk relates to ICT failure; this identifies existing controls, such as firewalls, anti-virus software and access controls, to mitigate threats to the Council's network.

b12. All ICT projects must have a project risk register in order to comply with PRINCE2 methodology adopted by the Council.

b13. The Information Risk Management Policy makes it clear InCOs are responsible for co-ordinating the information risk management process within their directorate. InCOs should review the results of risk assessments submitted by IAOs but IAOs interviewed were not aware of these assessments and are therefore unable to provide this assurance.

Recommendation: Ensure a formal information security risk assessment and management programme for all information assets on the Information Asset Register has been documented, is implemented by IAOs and regularly monitored and reviewed.

Management response: Accept.
This will be addressed as part of work outlined in response to recommendation a6.

Implementation date: 01 October 2014.

Responsibility: Information Governance Manager, Corporate Information Governance team.

b14. There is an internal audit planning cycle which takes account of areas of IG risk identified in Directorate and Service risk registers. Specific IG/DP risks have not recently been audited but IG compliance testing is embedded into areas of most audits. All internal audit reports go to both the Corporate Leadership team and the Corporate Governance and Audit committee.

b15. Internal Audit undertook a review of the IG department in 2009/10. A follow-up to this in 2011/12 showed most actions had been implemented or were 'work in progress'. One outstanding risk is that IAOs are not risk assessing information assets and reporting their findings to the SIRO.

Recommendation: Ensure on-going IG work continues to address actions identified in the 2011/12 Internal Audit follow-up review of the effectiveness of the IG team.

Management response: Accept.
The IG team will undertake a further review of this audit and will ensure any outstanding issues are programmed in to the work programme for next year.

Implementation date: 01 March 2014.

Responsibility: Executive Officer, Information Governance.

b16. A robust Information Security Policy (ISP) sets out the importance of information security and informs staff of their expected duties in relation to security. All employees interviewed were aware of the sensitivity of personal data and their responsibilities for protecting it.

b17. All IG policies have recently been reviewed and updated as necessary by IGMB and other relevant Council groups, and are endorsed by the SIRO. However, both the IS policy and DP policy provided for review did not have a review date on their cover sheet.

Recommendation: Ensure the cover sheet of all IG polices is completed with the latest review date.

Management response: Accept.
The IG team will co-ordinate work to check all policies and ensure the metadata is complete and up to date.

Implementation date: 31 December 2013.

Responsibility: Corporate Records manager, Corporate IG team.

b18. The ISP is mapped to the overarching IGF document and makes it clear it should be read in association with other IG policies, including the Password policy, Removable media / mobile computing policy and the Electronic Communications Code of Practice. However, the ISP does not name these policies or provide a link to them.

Recommendation: Ensure the ISP is linked to the relevant suite of IG policies to ensure staff are clear which policies are associated with it.

Management response: Accept.
The Council will ensure the ISP is linked to the relevant suite of IG policies.

Implementation date: 31 December 2013.

Responsibility: Corporate Records Manager, Corporate IG team.

b19. The Council maintain a comprehensive IT hardware asset register which details all PCs, laptops and mobile devices. Assets are tagged and bar-coded and suitable software is employed to manage the life-cycle of hardware and software assets, including owners, software license registration and applications installed.

b20. The Council allow staff to 'Bring Your Own Device' (BYOD) for certain smartphones, which, like all mobile media, are logged and managed centrally by the IT service desk.

b21. There is an on-going work programme 'Changing the Workplace' which introduces 'hot desking' and 'remote working'. Laptops have wireless networking enabled and a Virtual Private Network client to enable secure connection to the Council network when working remotely.

b22. The Council has a robust Information Security Incident Management Policy which contains details of what an information security incident is and details of security incident management procedures.

b23. There is a clear reporting mechanism for both DP and IT breaches with staff initially reporting to line managers who will then discuss severity with InCOs, who maintain a Directorate Breach Log. Serious incidents are immediately escalated to the IG Manager and Legal, who will make the decision on whether to inform the ICO.

b24. The IG manager is responsible for oversight of all Directorate Breach Logs and will work with Directorates to identify trends, record lessons learnt and formulate actions, if required. An annual breach report is provided to the SIRO.

b25. Staff interviewed were clear about the importance of reporting DP and IT breaches to their line manager.

b26. The Council are conducting a review of all 3rd party contracts to ensure that data protection requirements are appropriately specified. Guidance has been issued to managers to ensure DP and any other relevant IG requirements are specified in contracts.

Recommendation: Continue the review of all Council contracts to ensure that data protection requirements are appropriately specified within them.

Management response: Accept.
The new contract management framework (which incorporates data protection requirements) has been published and a corporate training programme is in development. The council will train all relevant staff and implement a system of checks on a sample of contracts to monitor whether data protection requirements are appropriately specified and contractors are being monitored within contracts.

Implementation date: 31 December 2015 (the corporate training programme is a 2 year programme).

Responsibility: Joint responsibility between Information Governance Manager (Corporate IG team), and Executive Manager (Legal and Commercial)

b27. The Council's standard 'terms and conditions' have been reviewed and specific indemnity clauses in relation to security breaches have been drafted. These include a clause to ensure 3rd parties promptly notify the Council of any breach of specified security measures.

b28. Contract monitoring arrangements are in the process of being strengthened and formalised. A series of templates and self-assessment questionnaires have been developed to assist in this area.

b29. The procurement process is also being strengthened and formalised to include a requirement to consult with technical experts where a project involves the creation of, or change to, IT systems. Guidance for the new process makes it clear that technically proficient staff are to be included at all stages of procurement where relevant.

b30. An internal audit report of the 3rd party contract for disposal of hardware assets identified three weak areas which have since been assessed and mitigated.

b31. Details of staff starters and leavers are monitored by HR and the SAP database is updated accordingly. SAP links directly to Microsoft's Active Directory (AD), which will automatically set up a basic user account to be active on the start date specified. A 'leaver action' on SAP will set a marker which informs ICT to close that login. The account is suspended immediately staff leave and after 30 days both email and Windows accounts are removed from the system.

b32. Passwords to the standard desktop environment are required to be complex in all cases, with up to 45 days before forced renewal. However, it was reported that passwords to access some databases, including Orchard and Paris, do not have a forced password change and consequently do not conform to the password management policy.

Recommendation: Review password access to all databases to ensure they comply with enforced change and complexity rules as required by the password management policy.

Management response: Partially accept.
The core password policy is applicable when accessing the majority of databases. In addition, the council deploys 'single sign-on' software to reduce the risks inherent in managing multiple passwords. The council will review databases where the password policy is currently not controlled by the core policy, and assess where improved password rules are required.

Implementation date: 01 July 2014.

Responsibility: IT Security Officer.

b33. User access is role based for the Academy and iClipse applications and can be limited to 'read only' screens in order to restrict access to sensitive personal data.

b34. Line managers are required to inform network administrators of starters and leavers but notification of staff who have moved departments is sometimes overlooked. Systems administrators in the Systems Support Team in Welfare and Benefits manage their own spreadsheets for inactive accounts. These are reviewed on a monthly basis, which should identify movers, but this is not as robust as it could be in identifying movers.

Recommendation: There is a risk that staff who have moved departments within the Council are not promptly removed from access to databases containing personal data which they no longer require. Ensure HR provide systems administrators with a list of staff who have moved departments to cross reference against staff access rights.

Management response: Accept.
The Corporate IG team will co-ordinate work to review current procedures and develop an action plan to address issues.

Implementation date: 01 October 2014.

Responsibility: Information Governance Manager, Corporate IG team.

b35. Periodic procedures are in place to confirm that database and system administrators still have an on-going entitlement to this role.

b36. If a member of staff has not logged into the Customer Relationship Manager (CRM) database for more than 3 months then access will be automatically denied. If this happens, staff have to be retrained in using the CRM system before access permissions are renewed.

b37. Encryption software has been applied to all portable media including laptops, pda's, usb memory sticks and smartphones.

b38. Portable devices are automatically updated with the latest anti-virus signatures when they are connected to the network.

b39. Only portable media on the Council's white-list i.e. trusted devices, can be connected to the network.

b40. Secure email transmission is available to all staff who have a GCSx account.

b41. The Council deploy email monitoring software to help prevent data loss, check for viruses and block inappropriate content.

b42. The Council are in the process of introducing software to ensure all GCSx email sent from the Council is subject to the Government's Protective Marking classification scheme.

b43. The Council have introduced an internally hosted secure file transfer system for sending restricted documents to organisations not on the GCSx network.

b44. Users’ ability to save data to the local (C) drive of laptops has not been revoked, although administrator rights are locked down.

Recommendation: Review the risks of laptop users being able to save data to their local C drive. This unstructured data is not automatically backed up and therefore may not conform to Council retention policies and is not searchable for information requests.

Management response: Accept.
The IG team will lead a review of the risks and benefits associated with laptop users being able to save data to local C drive. A report will be produced to be considered by ICT/IKM Liaison group, and any recommendations from this group will be communicated to IGMB.

Implementation date: 01 July 2014.

Responsibility: Information Governance Manager, Corporate IG team.

b45. The Council have a comprehensive Remote Working policy and staff are required to sign a home working agreement. The policy includes appropriate reference to information security requirements.

b46. Controls have been applied to protect the security of data in the homeworking environment. Remote access to corporate systems is via a secure Virtual Private Network (VPN) requiring two factor authentication.

b47. Staff working from home on a full time basis have received additional briefings on security, together with a home audit. Benefits appeals staff, who require appeals documents at home, are provided with lockable cabinets.

b48. Some agile Council staff carry manual paper files containing sensitive personal data which is taken home overnight. These staff do not appear to have been issued with lockable cabinets.

Recommendation: Ensure staff storing personal data at home are provided with a secure lockable cabinet as detailed in the Remote Working Policy.

Management response: Partially accept.
The Remote Working Policy outlines that the council will assess the work style of the employee and will provide equipment to enable access to LCC systems in accordance with the agreed workstyle. It specifies that a lockable cabinet should be in use where information is 'Restricted' or above, however it does not commit the Council to providing this equipment in all cases. The Council will ensure staff who are 'home based'- i.e. those who work from home as their main location - are provided with suitable lockable storage where required. Remote workers

who are not home based will not be provided with lockable cabinets by the council. To minimise/ reduce risks, employees are instructed to only take files out of the office which are actually needed, and to ensure that they are stored out of sight / securely. The Information Governance team will assess the consistency and adequacy of existing guidance regarding taking files home, and security at home and in transit. Guidance will be reviewed and amended if necessary.

Implementation date: 01 May 2014.

Responsibility: Information Governance Manager, Corporate IG team.

b49. Staff are allowed to use approved smartphones to access the Council network. Email and calendar services are provided over a secure encrypted connection. This is managed by the ICT service desk, who have the ability to remotely wipe devices if they are lost.

b50. There are robust network controls and procedures in place to ensure that the confidentiality and integrity of personal data is maintained. Anti-virus, firewalls and operating systems are effectively maintained by the ICT Server Team and the security team, and security vulnerabilities are promptly acted upon. Vulnerabilities are reported at management team meetings.

b51. Intrusion Prevention Systems have been deployed on the network and are regularly monitored. In addition, Data Loss Prevention (DLP) software is used to ensure end point control.

b52. The network is subject to regular health checks and penetration testing by both in-house staff and independent 3rd parties.

b53. Network and system settings are subject to rigorous change control procedures and the effectiveness of these procedures is tested and monitored. Audit logs are enabled on the corporate network and also routinely monitored.

7.3 The agreed actions will be subject to follow up to establish whether they have been implemented.

7.4 Any queries regarding this report should be directed to Chris Littler, ICO Good Practice.

7.5 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of working practices, policies and procedures. The following staff member was particularly helpful in organising the audit:

Andrew Nutting – Executive Officer, Information Governance Department.