APPENDIX 1

Southend-on-Sea Borough Council

Data protection audit report

Executive summary
February 2013

ico.
Information Commissioner's Office

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 Southend-on-Sea Borough Council agreed to a consensual audit by the ICO of its processing of personal data in December 2011.

1.4 An introductory teleconference was held on 17 September 2012 with representatives of Southend-on-Sea Borough Council to identify and discuss the scope of the audit and after that on 30 October 2012 to agree the schedule of interviews.

2. Scope of the audit

2.1 Following pre-audit discussions with Southend-on-Sea Borough Council it was agreed that the audit would focus on the following areas:

c. Records management (manual and electronic) – The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records. This will include any policies and procedures in place that govern how personal data is processed, and reporting lines to ensure corporate awareness of issues.

d. 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.

e. Requests for personal data – The procedures in place to deal with any requests for personal data. This will include requests by individuals or their representatives for copies of their personal data and any data sharing agreements.

3. Audit opinion

The purpose of the audit is to provide the Information Commissioner and Southend-on-Sea Borough Council with an independent assurance of the extent to which the Council, within the scope of this agreed audit is complying with the DPA.

The recommendations made are primarily around enhancing existing processes to facilitate compliance with the DPA.

Overall Conclusion	
Reasonable assurance	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements. We have made two reasonable assurance and one high assurance assessment where controls could be enhanced to address the issues summarised below.

4. Summary of audit findings

Areas of good practice

The Directors and Heads of Service sign-off an annual Manager Assurance Statement that assesses risk by service area. The statement covers data quality and security risks and provides an integrated way of informing the internal audit plan. The Manager Assurance Statements are also reviewed by the Corporate Management Team.

Auditors were pleased to observe that a major data security awareness programme, 'TH!NK PRIVACY', has been launched at the Council using a variety of media.

An un-redacted and redacted version of personal data compiled in response to subject access requests is retained by the Council. This is good practice as it provides a complete audit trail of the response issued to each requester and will assist the Council in answering any redaction related enquiries.

Areas for improvement

There is no corporate protective marking scheme in use at the Council for electronic or paper documents.

The Council should introduce endpoint control for CD's and USB's through the implementation of the acquired SOPHOS software as an information security priority.

The Council should deliver periodic subject access refresher training for staff involved with the handling of personal data in their service area.

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 Southend-on-Sea Borough 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.

Southend-on-Sea Borough Council

Data protection audit report

Information Commissioner's Office

Auditors:	Leanne Doherty (Audit Team Manager) Aideen Oakes (Engagement Lead Auditor) David Simmons (Lead Auditor)
Data controller contacts:	Indi Viknaraja – Information Governance Officer
Distribution:	Indi Viknaraja – Information Governance Officer Rob Tinlin – Chief Executive
Date issued:	**21 February 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 Southend-on-Sea Borough 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 page 4

2. Scope of the audit page 5

3. Audit opinion page 6

4. Summary of audit findings page 7

5. Audit approach page 8

6. Audit grading page 9

7. Detailed findings page 10 - 32

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 Southend-on-Sea Borough Council agreed to a consensual audit by the ICO of its processing of personal data in December 2011.

1.4 An introductory teleconference was held on 17 September 2012 with representatives of Southend-on-Sea Borough Council to identify and discuss the scope of the audit and after that on 30 October 2012 to agree the schedule of interviews.

2. Scope of the audit

2.1 Following pre-audit discussions with Southend-on-Sea Borough Council it was agreed that the audit would focus on the following areas:

c. Records management (manual and electronic) – The processes in place for managing both electronic and manual records containing personal data. This will include controls in place to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records. This will include any policies and procedures in place that govern how personal data is processed, and reporting lines to ensure corporate awareness of issues.

d. 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.

e. Requests for personal data – The procedures in place to deal with any requests for personal data. This will include requests by individuals or their representatives for copies of their personal data and any data sharing agreements.

3. Audit opinion

3.1 The purpose of the audit is to provide the Information Commissioner and Southend-on-Sea Borough Council with an independent assurance of the extent to which the 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	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements. We have made two reasonable assurance and one high assurance assessment 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 Directors and Heads of Service sign-off an annual Manager Assurance Statement that assesses risk by service area. The statement covers data quality and security risks and provides an integrated way of informing the internal audit plan. The Manager Assurance Statements are also reviewed by the Corporate Management Team.

Auditors were pleased to observe that a major data security awareness programme, 'TH!NK PRIVACY', has been launched at the Council using a variety of media.

An un-redacted and redacted version of personal data compiled in response to subject access requests is retained by the Council. This is good practice as it provides a complete audit trail of the response issued to each requester and will assist the Council in answering any redaction related enquiries.

4.2 Areas for improvement

There is no corporate protective marking scheme in use at the Council for electronic or paper documents.

The Council should introduce endpoint control for CD's and USB's through the implementation of the acquired SOPHOS software as an information security priority.

The Council should deliver periodic subject access refresher training for staff involved with the handling of personal data in their service area.

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 Southend-on-Sea Borough Council Civic Centre between 13 and 15 November 2012.

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	The arrangements for data protection compliance with regard to governance and controls provide a high level of assurance that processes and procedures are in place and being adhered to. The audit has identified 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.
	Reasonable assurance	Low priority	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements.
	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The audit has identified scope for improvement in existing arrangements
	Very limited assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

7. Detailed findings and action plan

Findings flowing from the audit will be risk categorised using the criteria defined in Section 6. The rating will take into account the impact of the risk and the probability that the risk will occur.

7.1 Scope C: 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. This will include any policies and procedures in place that govern how personal data is processed, and reporting lines to ensure corporate awareness of issues.

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.

c1. The Corporate Director of Support Services is also the appointed Senior Information Risk Owner (SIRO) and reports to the Chief Executive (CE). The SIRO accepts overall responsibility for information governance at the council.

c2. There is a centralised Data Protection function at the council that falls within the remit of the Information Governance Team. The Information Governance Team reports to the SIRO on data protection matters.

c3. The Information Governance Team is led by a Group Manager who has oversight for ensuring compliance with the Data Protection Act 1998 (the DPA) and has overall oversight of records management.

c4. The Information Governance Officer (IGO) post holder undertakes the tasks required to help the council comply with the DPA at an operational level which includes records management responsibilities for example records relating to subject access requests.

c5. Heads of Service accept delegated responsibility from the SIRO in relation to Information Asset Ownership, however it was reported at interview that the Information Asset Owner (IAO) role had not yet been thoroughly embedded. Heads of Service interviewed did not recall receiving any tailored training for their IAO role.

Recommendation: Ensure Heads of Service are aware of their responsibilities as IAO i.e. that they understand what information is held in their service, how it is used and transferred, and who has access to it and why. This could be achieved by including IAO responsibilities into relevant job descriptions and providing specific IAO role based training on an annual

basis. Please see '*Local Public Service Data Handling Guidelines, version 2, August 2012*'.
Management Response: The Council will revise the Terms of Reference of the Overarching Information Management Strategy to include IAO, Caldicott Guardian and SIRO duties. Job descriptions for Heads of Services will be revised to include their IAO and DP responsibilities. One Senior Leadership Team Meeting each year will cover a session on the roles and responsibilities of IAOs.

Implementation Date: Nov 2013
Responsibility: SIRO

c6. It was reported at interview that an Information Governance Steering Group, attended by the SIRO and Heads of Service meets two to three times annually to agree information governance strategy.

c7. The council has an Audit Committee and a Corporate Risk Management Group tasked with identifying and monitoring risks, including those relating to records management.

c8. There is an overarching records management policy in place at the council with an owner and designated review cycle. The Records Management Policy is supported by the Data Protection Policy, the Corporate Information Security Policy and other supplementary guidance.

c9. At present a corporate protective marking scheme is not in use for electronic or paper documents containing personal data.

Recommendation: Adopt the government protective marking scheme or equivalent in all directorates. Monitor the scheme's implementation and use.
Management Response: At present the Council does apply a marking system to all Reports to Council and Committees. We will now consider whether the Government Protective Marking Scheme (GPMS) can be introduced, either wholly or partly and will also consider the practicalities around the implementation. In addition, as the Cabinet Office is currently conducting a review of the GPMS to simplify it to three tiers (Official, Classified and Top Secret) the Council will continue to closely monitor how this new initiative unfolds as this will have an impact on any proposed implementation.

Implementation Date: Dec 2014
Responsibility: SIRO

c10. The IGO delivers an overview of data protection at staff induction including the data quality principles that relate to the adequacy, relevancy, accuracy and retention of personal data. The IGO also delivers an optional corporate data protection training session that includes aspects of records management. In addition, some directorates deliver their own training on data protection related subjects, for example; Children and Learning Specialist Services deliver annual training on information sharing to social work staff. The IGO also

provides mandatory training for teams that have been subject to a data breach. However the Director of Support Services reported that they had not completed any specialist training for their role as SIRO and had not yet subscribed to the National Archives SIRO Newsletter. The council could therefore utilise other readily available online training resources to supplement its existing training programme.

Recommendation: All staff with records management responsibilities should complete level 1 HMG Cabinet Office Protecting Information e-learning module or equivalent as part of their mandatory training. The SIRO should register with the National Archives and subscribe to the monthly SIRO newsletter. The SIRO and IAOs should consider completion of HMG Cabinet Office Protecting Information Training levels 2 and 3.
Management Response: Whilst the SIRO has not completed HMG Cabinet Office Protecting Information Training, it should, however, be noted, that the SIRO has over 15 years of experience working in information governance and was responsible for setting up the first Social Care and Health information sharing protocols in the London Borough of Tower Hamlets, that went on to form the base of wider London agreements. The SIRO has been registered with the National Archives and subscription has been arranged for the monthly newsletter. As noted by the auditors the Council has an extensive training programme dealing with DP. The training programme scheduled for the coming year will have a focus on Records Management.

Implementation Date: Dec 2013
Responsibility: SIRO

c11. Staff interviewed demonstrated awareness of the mandatory online 'spark' e-learning data protection module authored by the IGO and reported that it covered the secure storage of records. It was noted that staff handling personal data have not been issued with a deadline to complete this training.

Recommendation: Select a practical deadline for all staff handling personal data as part of their job role to complete the mandatory online 'spark' data protection e-learning module. Completion of the module should be monitored and evidenced by service area.
Management Response: A completion timeline of August 2013 has been agreed.

Implementation Date: Aug 2013
Responsibility: Indi Viknaraja

c12. A number of records management related resources are available to staff on the intranet, for example; the council's Records Management Policy. Key data protection messages are also communicated to staff at induction, via Team Brief and the 'Highlight' newsletter.

c13. Staff interviewed demonstrated an awareness of the importance of ensuring that customers understood why their data was being collected by the council,

how it would be used and with whom it would, or might, be shared.

c14. Fair processing information is drafted by DP-Co-ordinators for use in their service area.

c15. There was evidence that Children and Learning supply a privacy notice at the start of their relationship with a family entitled: '*What Information Children's Social Care hold about your family and how you can apply to see it.*' There was also evidence that Revenues and Benefits include fair processing information and obtain consent in forms used to collect customer personal data. To assist in drafting and maintaining consistent fair processing notices and statements we would suggest that the council produces guidance based on the ICO's Privacy Notices Code of Practice and considers implementing overarching procedures that periodically refresh consent.

c16. Fair processing information concerning call recording is supplied to customers who contact the council using the Customer Service Centre Helpdesk.

c17. The Customer Service Support and Administration Team receive and scan postal correspondence centrally. The post is sorted and scanned onto the council's electronic document records management system (EDRMS) 'Civica' by service area. Hard copy postal correspondence is securely retained for a three month period before destruction, unless the hard copy document has been passed directly to the team it relates to for legal reasons.

c18. Interviewees explained that the Customer Services Support and Administration Team also facilitate the submission and recall of records from archive.

c19. Responsibility for the preparation of records for transfer to external archive is the obligation of each service area. Service areas fill up archiving boxes and attach unique barcodes to the outside of each box and then complete a data transfer sheet detailing destruction/review dates, bar code and brief details of the box contents. Each service area maintains an independent log of its own archiving and the use of box barcodes can be monitored by the Support and Administration Team. In addition any service wishing to archive records will be asked to complete a new depositor's checklist which enables the Support & Administration Team to monitor who would be allowed to view records should they be recalled.

c20. The council is able to reconcile the number of archive boxes collected and deposited into archive with its contractor. This is achieved by the contractor cross-referencing unique box barcodes against entries made on their system by the council. The reconciliation process is repeated at delivery to off-site storage.

c21. When an individual record is extracted from a recalled archive box it is the responsibility of that service area to update its archive log and the box data transfer sheet if the individual record is to be kept and the box returned to archive.

Recommendation: It is recommended that the council review this part of the recall process. Consider both the secure storage of the recalled archive box once it has been retrieved by the service area that requested it and how to ensure the accuracy of both the archive log and data transfer sheet.
Management Response: Data transfer sheets are kept and stored electronically in Civica. Responsibility for changes that take place within the recalled boxes remain with the service areas. An updated data transfer sheet must be supplied by the service prior to the recalled box being returned to the site.
Accordingly procedures have been amended and staff reminded of their responsibilities.

Implementation Date: March 2013
Responsibility: Karen Wright

c22. During interview auditors were informed about the existing 'Carefirst' system quality assurance process and an initiative to help improve the accuracy of information stored on Carefirst called 'key information checker'. It was explained that a customer's 'key information sheet' is accuracy checked and used to update that client's assessment. The key information sheet is completed by a social worker and reviewed on a quarterly basis. The checker helps social workers maintain and improve the accuracy of customer information on Carefirst. It was reported that Revenues and Benefits also have quality assurance checks, such as SHBE (Single Housing Benefit Extract) which the DWP match to their records providing Benefits with a list (HBMS – Housing Benefit Matching Service) that staff refer to.

c23. It was reported at interview that social workers maintain their own notebooks and paper based assessments which they use to collect personal information when offsite and bring back to update Carefirst. Once information has been entered into Carefirst the assessments are disposed of in confidential waste bins. Transporting hard copy personal data offsite poses a recognised data security risk, to help mitigate this risk all social work staff abide by professional standards covering customer confidentiality.

Recommendation: Implement a process to ensure that only essential information is recorded by social workers in notebooks and paper assessments when offsite, and require staff to obtain manager authorisation if they want to take sensitive information offsite for other purposes.
Management Response: Much of the social work activity is recorded directly into Carefirst. With the increased use of tablets/laptops the risk of transporting paper documents is reduced. As more social workers move to mobile working additional guidance and support will be given to ensure best practice continues in keeping personal data confidential and secure. Where it is necessary to take personal data off site, this will be done in line with the Council's procedures, which includes carrying them in lockable cases.

Implementation Date: April 2013
Responsibility: Catherine Cobb/Ed Spacey

c24. The council has an overarching corporate retention schedule. The corporate schedule is supported by 20 service area retention schedules specific to the records held in that area. The documented retention schedules for all service areas can be accessed by staff via the intranet.

c25. The council's Records Management Policy references business continuity and disaster recovery in relation to manual and electronic records. It explains that such risks are considered in the council's risk management regime.

c26. The Revenues and Benefits service area uses the council's on site reprographic data processor OCE to print, pack and post high volume customer correspondence.

c27. The council operates CCTV systems in its public areas and at entry and exit points for security purposes. The CCTV images are stored on a hard drive and retained for 17 days. In addition, calls received by the council's Customer Service Centre are recorded.

c28. It was explained at interview that there is an information asset register for hardware and software assets but a corporate information asset register for physical records containing personal data is not currently maintained.

Recommendation: Create an information asset register for physical assets storing personal data. Allocate responsibility for maintenance of physical information assets to the relevant IAOs. All information assets should be updated, reviewed and risk assessed on a periodic basis.
Management Response: In significant areas of the Council, example Revs and Bens and HR/Payroll all information is held electronically and as such there is no requirement for an asset register. The IGO will hold a corporate physical assets register which will be reviewed annually.

Implementation Date: Dec 2013
Responsibility: All areas/Indi Viknaraja

c29. Policies and guidance in relation to the secure storage of records are outlined within the Corporate Information Security Policy and Records Management Policy.

c30. Although it was reported that the council does not follow a documented visitors policy, auditors were required to sign-in at reception each day and were issued with a visitor pass by the Facilities Team. Auditors were collected from reception and escorted into the main building by a member of staff.

Recommendation: Produce a visitor policy for Facilities and other staff to follow, outlining their obligations and responsibilities in relation to external visitors.

Management Response: The Council has an existing Security Policy which includes procedures (as listed below) which must be followed with regards to the visitors to the Civic Centre.
All Members and staff are issued with identity cards that must be worn visibly at all times.
Members and staff are advised to remain vigilant at all times.
Members and staff are encouraged to politely challenge unscheduled visitors and suspicious situations within and around the premises.
A visitor's register is kept at the CSC reception and visitors are issued with a visitor's badge which must be worn at all times and returned upon departure.
Staff are informed when visitors have arrived and it is their responsibility to collect the visitor from reception, escort to their destination and return to reception.

Implementation Date: Complete
Responsibility: Karen Wright

c31. Hot-desking and a clear desk culture is in operation at the council. Adherence to clear desk is monitored by managers who conduct periodic spot checks using red, amber and green cards to flag poor compliance.

c32. Access to the council's network can only be obtained by logging in with a user name and password. Similarly access to the Carefirst and Northgate systems is password controlled with the level of access granted dependent on a user's access permissions.

c33. Staff may apply to homework, but their application must be approved at line management level and they must complete the mandatory 'spark' online data protection e-learning module before approval for homeworking will be given.

c34. There is a data security breach management procedure in place. All DPA breaches should be reported centrally to the IGO. The IGO maintains a data security breach log of all incidents reported. The decision on whether to report a data protection breach to the ICO is taken by the SIRO.

c35. It was reported at interview that Revenues and Benefits do not have lockable wall mounted key safes in which to securely store filing cabinet, locker and pedestal keys. Additionally it was revealed that employees keep locker keys on their person during working hours and take them home at night. It was discovered that lockers are sometimes used to temporarily store documents containing personal data.

Recommendation: Install lockable wall mounted key safes in service areas processing personal data, so that cabinet and pedestal keys can be securely stored in the same location. Allowing employees to take locker keys home overnight poses a data security risk, particularly if lockers are used to store personal data and so the Council should instruct employees to store locker keys in key safes overnight.

Management Response: There are key safes already in place in most service areas, to include Revs and Bens, HR, various teams in ACS and Finance, Legal and Democratic Services and C&L. In areas where key safes are required they will be put in place. As a part of the ICO Audit feedback all staff have been reminded that Council papers should not be stored in personal lockers.

Implementation Date: June 2013
Responsibility: Karen Wright/Indi Viknaraja

c36. The council has a dedicated policy detailing procedures for the disposal of confidential waste, supplemented by directorate level guidance such as the Children and Learning Disposal and Archiving procedure.

c37. Auditors observed locked confidential waste bins situated on each floor of the Civic Centre. A contractual arrangement is in place for the collection and disposal of confidential waste by a third party. Weekly confidential waste destruction certificates are received by the council.

c38. An agreement is in place for the off-site storage of archived manual records. The agreement covers the destruction of archived records when they reach their retention deadline. Service areas that wish to review their records prior to destruction are contacted by the Customer Services Support and Administration Team prior to the records reaching their destruction deadline.

c39. There is currently no archiving and deletion solution on the Northgate system. It was reported that Northgate has been in use by Revenues and Benefits for approximately five years and that personal data stored on Northgate has not yet reached its retention deadline. It was also reported at interview that there were similar issues with archiving and deleting records on Carefirst. There is a project plan in place to address the issues with Carefirst.

Recommendation: It is recommended that the council implement and complete a project plan to deliver archiving and deletion solutions for both Northgate and Carefirst to ensure future adherence to retention schedules.
Management Response: In Nov 2012, ACS agreed that all relevant records on Carefirst, as defined by the document retention policy would be locked down and in following 12 months deleted. A number of technical issues have caused a delay in the implementation, but it is anticipated that it will be resolved shortly and the review of the deletion process will then be initiated. The archiving solution within Northgate risks corrupting the entire database. So as things are currently, we will not be looking to implement archiving within Northgate. If and when Northgate can alter their system to facilitate archiving, the Council will look to implement.

Implementation Date: July 2013 (for Carefirst)

Responsibility: Christine Lynch, Veronica Dewsbury (Northgate) Catherine Cobb , Ed Spacey (Carefirst)

c40. Within the Children and Learning Directorate it was reported that monthly audits of a sample of records stored on Carefirst are conducted by line managers. These audits cover aspects of records management, for example; the accuracy and relevancy of personal data recorded in the files. The audit results are reported to the Social Care Management Group and in turn to the Departmental Management Team (DMT) twice a year.

c41. It was discussed at interview that there are a number of reporting tools that could be used more extensively to assess the council's records management performance, for example; a monthly report on records due for destruction compiled by the Customer Services Support and Administration Team. Similarly the SIRO report produced in June 2012 references the requirements of the Local Public Services Data Quality Guidelines as good practice targets, and the monthly Support Service Performance Report includes subject access and information security breach statistics distributed to DMT.

Recommendation: Collate and review monthly reports in relation to archiving and destruction, to help avoid retention and destruction errors. Include records management related key performance indicators in the monthly Support Services Performance Report and future annual SIRO reports.
Management Response: With electronic records the new system will include retention and destruction and the ability to report. With regards to the existing system there are some limitations, example with Carefirst we are working around. With regards to hard copy records, the Council undertook a major exercise to destroy requisite files as a part of the refurbishment. This provides a good base for moving forward. Where records are stored off-site the Council will, in future, provide quarterly reports to show proper destruction of files. This will be reported as a part of the Support Services Performance Indicator regime.

Implementation Date: March 2013
Responsibility: Karen Wright, Catherine Cobb, Indi Viknaraja

c42. Directors and Heads of Service sign-off annual Manager Assurance Statements that assess risk within their service area. The statement covers data quality and information security risks. The statements inform the internal audit plan and are reviewed by the Corporate Management Team (CMT).

c43. The council's Head of Internal Audit reported that as part of their work the Internal Audit Team would consider including an aspect of information management or data protection in audit reviews where it was considered to be a key risk. The council could include data protection / records management

as a standard stand-alone item on the internal audit plan to ensure regular DPA compliance checks are completed

7.2 Scope D: Security. 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.

d1. The council has adopted an information security framework designed to meet external requirements including the government GCSx Code of Connection requirements for connection to government secure network.

d2. Other external requirements include compliance with controls set for connection to the NHS N3 network and access to the Department for Work and Pensions (DWP) benefits database.

d3. The council have adopted the ITIL standards for IT service management and this is reflected in IT policies.

d4. The GCSx Code of Connection and ITIL map to the ISO27002 Code of Practice but the council have not adopted an associated formal Information Security Management System required for any ISO27001 accreditation.

d5. The SIRO has introduced a data protection strategy and dedicated Information Governance posts supported by service area based DP Co-ordinators who can provide data protection expertise for local projects.

d6. The council has a Risk Management Policy Statement and Strategy supported by the Risk Management Toolkit. Risks are identified and documented in service level risk registers which feed the corporate risk register. The corporate risk register incorporates risks relating to information management.

d7. The council audit plan reflects identified risks with external specialist IT auditors employed to check information security (IS) controls.

d8. High risk programmes relating to personal data processing have been identified including Public Health transfers, the 'Troubled families' programme and Local Welfare Assistance benefits changes.

d9. Project teams have been established to manage these programmes with board level sponsors. These projects have their own risk registers.

d10. There is a regularly updated Corporate Information Security Policy owned by the SIRO which also clearly states the SIRO responsibilities.

d11. The council have a high level ICT Infrastructure Policy which reflects GCSx Code of Connection control requirements.

d12. Specific controls such as the password policy refer to network access rather than being overarching and applying to all systems used such as the social services Carefirst application.

Recommendation: The Information Security Policy should apply to all systems and applications used to process personal data.
Management Response: The Corporate Information Security Policy does cover all systems and all users – an extract below may assist. The fact that administration of some systems such as Carefirst are managed at business level does not mean that they do not comply with the Policy. Those who are granted access to Information and information systems must:

Only access systems and information, including reports and paper documents to which they are authorised.

Use systems and information only for the purposes for which they have been authorised.

Comply with all applicable legislation and regulations.

Comply with the controls defined by the Information Asset Owner.

Comply with all Southend-on-Sea Borough Council Policies, Standards, Procedures and Guidelines, along with the policies and requirements of other organisations when granted access to their information.

Not disclose confidential or sensitive information to anyone without the permission of the Information Asset Owner, and ensure that sensitive information is protected from view by unauthorised individuals (e.g. public places).

Keep their passwords secure, not allowing anyone else to use their account to gain access to any system or information.

Protect information from unauthorised access, disclosure, modification, destruction or interference.

Not attempt to disable or bypass any security features which have been implemented.

Notify your Line Manager of any actual or suspected breach of Information Security, or of any perceived weakness in the organisation's Security Policies, Procedures, Practices, Process or Infrastructure in accordance with the Data Security Breach Procedure.

Implementation Date: Complete
Responsibility: Kim Karacolak

d13. Procedures exist to identify ICT assets and a central register of ICT assets is maintained. Details registered include personal data processed, staff numbers with access and any remote access.

d14. The Manager's Assurance Statements include data protection requirements including safe disposal compliance. The council should consider providing regular data protection compliance reports to Information Governance and reporting results within the Manager's Assurance Statement.

d15. It was reported that the IT hardware asset register is not up to date. The council intends to update the IT asset register as a requirement for setting up an endpoint control 'Whitelist' of approved devices.

Recommendation: Implement procedures to ensure regular and accurate updating of the IT asset register.
Management Response: We have been auditing mobile devices such as laptops and will be updating our IT asset register.

Implementation Date: August 2013
Responsibility: Kim Karacolak

d16. There are no proposals to identify any unofficial devices such as USB memory sticks existing on council premises.

Recommendation: The council should consider implementing a memory device 'amnesty' so as to collect any redundant media in line with policies adopted by other local authorities when implementing endpoint control systems.
Management Response: The Council plans to introduce methodology and technology to only allow registered and encrypted removable media. This will be introduced through a staged process that will allow measures to be put in place over an agreed period of time to ensure minimal operational impact to the business.

Implementation Date: November 2013
Responsibility: Kim Karacolak

d17. The Manager's Assurance Statement includes a requirement for compliance with the breach process.

d18. A major data security awareness programme, TH!NK PRIVACY, has been launched at the council using various media.

d19. The IGO delivers an overview of data protection to staff at induction including the seventh principle. The IGO also delivers optional corporate data protection training sessions to staff that include aspects of technical and organisational security.

d20. A dedicated intranet area has been created for use by the Information Governance Team and DP-Co-ordinators covering areas of good practice as well as regular ICO press releases.

d21. Members of the Information Governance Team are trained up to BCS ISEB Certificate level for Data Protection and Freedom of Information (FOI) and Senior IT managers have been trained at ITIL Foundation level.

d22. Standard contracts employed for third party services have confidentiality requirements referencing the DPA.

d23. The council has carried out on site checks of suppliers including Thames Security Shredding and Meritec.

d24. The web service contract with Jadu makes specific reference to a requirement to protect against common IT threats including SQL Injection and XSS.

d25. Essex County Council provide the social work emergency team service but are provided with only limited access to the Carefirst social work service, relying on the council's duty social worker to provide any detailed information if required.

d26. The Incident Reporting Policy covers the process for confidential waste disposal by third party contractors and any security breaches are required to be reported back to the council.

d27. The council is currently in the process of reducing the number of office buildings used to three. The Civic Centre and one other employ G4S Symmetry software to control access through proximity cards.

d28. Staff swipe card zones are configured to restrict access to high security areas such as the IT Server room. However in general, security is restricted to the perimeter with no additional swipe access doors in lift lobbies. Swipe cards restrict access on the basis of zone and time with default set 07:00 to 19:00 normal office times.

d29. The Civic Centre provides public access to the general enquiry desk, Registrar Office as well as the canteen and café area. The lobby also provides the main entrance for council staff to office areas.

Recommendation: Additional security should be provided reflecting the approach of other councils with similar civic centres. Options include installing turnstiles at the lobby entrance.
Management Response: Installing turnstiles will now form part of the new ground floor layout to be implemented in the next phase of the Civic Centre refurbishment. For additional security the Council is also considering changing CCTV for improved images and restricting access to points of access during out of office hours.

Implementation Date: March 2014
Responsibility: Martin Musgrave/Karen Wright

d30. A contract exists to recycle or dispose of redundant IT media with CESG approved over-writing software used prior to this.

d31. At the Civic Centre staff now make use of multi-function devices (MFDs) for printing and scanning. The maintenance contract for these complies with standard confidentiality requirements but although these devices contain hard disk drives the process for any movement off-site does not appear to comply with the IT Media Policy.

Recommendation: MFDs should be treated as PCs in terms of security policies with disks over written if leaving council premises in line with the IT Media Policy.
Management Response: Rejected - the printers work on the basis of 'print and delete'. In addition, the data is automatically deleted on a pre-set time line e.g. 24 hours. For equipment that is taken away e.g. MFD's these are either wiped or destroyed, dependent upon whether the equipment is to be recycled.

Implementation Date: Rejected
Responsibility: n/a

d32. The process for starters, leavers and movers relies upon line managers completing a standard form which for starters also lists applications requested.

d33. The IT Service desk will arrange for any network access while major social care and benefits systems have their own controllers to authorise access, based on criteria including job roles and completion of their system training.

d34. At present temporary / contractor accounts without end dates are picked up through quarterly inactivity reports run by the Service Desk. Where contract duration is not supplied accounts are processed as if for permanent staff.

Recommendation: Requests for temporary / contract staff should include the contract duration so that this can be included in the network account set-up with duration time included in the Active Directory setting. A default time duration reflecting minimum contract times should be used if no time is defined by requesting managers.
Management Response: This will be implemented immediately.

Implementation Date: Feb 2013
Responsibility: Kim Karacolak

d35. The Service Desks and Application Controllers are supplied with retrospective monthly leaver's reports from HR payroll to identify any leavers not reported by line managers. No process exists to report failures by line managers to notify.

Recommendation: Any failure by line managers to notify IT of staff leavers should be treated as a security incident and reported to the Information Governance Team.
Management Response: A leaver's checklist for managers is produced by HR. This is a form managers complete and send to HR when an employee leaves. Although this is for HR purposes it

will be amended to remind managers that they must ensure ICT and facilities are advised to cancel their access to ICT systems and their ID card within a prescribed time. It will also impress that for managers who fail to do so it will be logged as a security incident which will be reported to the SIRO.

Implementation Date: August 2013
Responsibility: Kim Karacolak, Sue Putt

d36. The Service Desk manages the suspension of network access for employees on long term sick or maternity via regular inactivity reporting. The council should consider amending this approach to include line manager or HR notification and authorisation for employee access suspension to ensure this is actioned in a timely and accurate manner.

d37. The council's network and network password rules meet GCSx Code of Connection requirements using for example EAL4 Certified Firewalls.

d38. Users access the network using a combination of thin client, PC and laptop devices.

d39. Personal computers and laptops have a standard build which enables the use of CD and USB drives.

d40. SOPHOS software has been purchased by the council but the endpoint capability has yet to be implemented to control CD and USB use.

Recommendation: The introduction of endpoint controls should be treated as a security priority. Until then additional awareness campaigns will be required to reduce risks.
Management Response: Endpoint controls are to be introduced by the end of March.

Implementation Date: March 2013
Responsibility: Kim Karacolak

d41. Various systems are in place such as Proofpoint to provide secure use of email including scanning to detect both malware and phishing attacks.

d42. Remote working arrangements meet GCSx requirements with all laptops encrypted using Bit Locker and Tru-crypt with secure VPN gateway use.

d43. Application access for remote VPN users is controlled by use of a Citrix gateway which in turn is supported by use of a CISCO VPN concentrator to provide additional security.

d44. Blackberries are used by some staff but these are controlled using the council's own Blackberry server.

d45. The council has a contract with third party supplier 'Encription' to provide system penetration tests so as to meet GCSx connection requirements. This covers requirements such as CESG Manual Y compliance for wireless LAN.

d46. These tests have now been extended in terms of scope to cover elements of 'social engineering' penetration threats such as unauthorised access to buildings and attempted use of network ports.

d47. The tests have not covered high risk areas such as attempts to obtain personal data from Customer Service staff either at the public helpdesk or via the Customer Service Centre Helpdesk.

Recommendation: Social Engineering penetration tests should cover high risk areas such as the Customer Service Centre Helpdesk.
Management Response: The Council will have another test carried out by the end of this year.

Implementation Date: Dec 2013
Responsibility: Kim Karacolak

d48. ITIL standards are applied to OS and AV updates with WSUS used to update Microsoft software and processes in place to cover Unix requirements.

d49. Third parties such as JadU have been employed to provide expertise and maintenance for the council's web-based services.

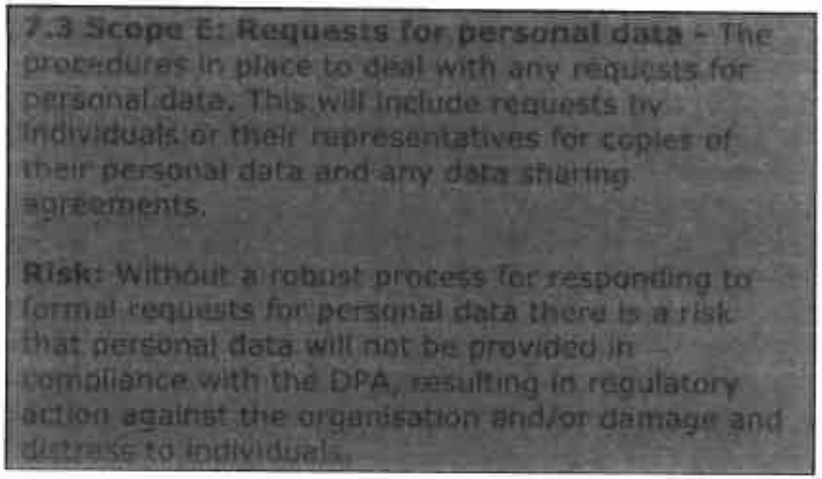
d50. Online payment services are provided by Capita using their own secure site.

d51. The Information Governance Team has produced a Privacy Impact Assessment (PIA) process and guidance which has been trialled with information governance nominated contacts.

d52. The PIA process will require formal sign-off as a mandatory project requirement but this has yet to be achieved.

Recommendation: Sign-off and formal adoption of the PIA process should be treated as a priority.
Management Response: The PIA process is covered in the Project Management Guidance which has already been commissioned. This is a 2 part document which comprises the detailed guidance and the Quick User Guide. Sign off and roll out to be carried out before June.

Implementation Date: June 2013
Responsibility: Indi Viknaraja



e1. There is a Data Protection Policy in place at the council that covers the right of subject access. This is supported by supplementary guidance including the Principle 6 and Subject Access Request Procedure. All policies and guidance are made available to staff on the council intranet.

e2. There is a single gateway approach to directing subject access requests at the council with accessible information on the council's website advising the public what they need to do to make a request for their personal data.

e3. The council's data protection function including the processing of subject access requests is managed in the Support Service Directorate by the Information Governance Team.

e4. The IGO is the key post holder with overarching responsibility for the operational handling of subject access requests.

e5. The IGO is supported by DP-Coordinators who administer requests for personal data in their service area. The collation and redaction of personal data to respond to subject access requests is generally handled by the DP-Co-ordinators.

e6. The Children and Learning Directorate receives the largest number of requests at the council, because of this it has a unique Access to Records Assistant post to assist with locating personal data for requests and making redactions.

e7. The IGO has responsibility for the delivery of internal data protection training. The IGO delivers a brief overview of data protection at staff induction including the sixth principle. The IGO also delivers an optional corporate data protection training session that includes a section on accessing personal information. In addition, some directorates deliver their own training on data protection related subjects, for example; Children and Learning Specialist Services deliver annual training on information sharing to social work staff.

e8. A training completion log is maintained by the IGO in relation to the data protection 'spark' e-learning module. In order to maintain an accurate training log the DP-Coordinators report to the IGO when a staff member successfully completes the module in their

service area. Consider the feasibility of an automatic training completion notification sent straight to the IGO to help ensure that the training log is kept up to date.

e9. Additional data protection training has been supplied by the IGO to the council's DP-Coordinators. The IGO and DP-Coordinators attend six weekly meetings that provide a regular forum for the discussion of complex subject access requests. It was unclear at interview if formal subject access refresher training is conducted for all staff and if so how frequently this takes place.

Recommendation: It is recommended that the council deliver periodic refresher training, covering aspects of subject access, to those staff handling personal data.
Management Response: Since the IGO was appointed in August 2008, 2 refresher training sessions have been conducted for Co-Ordinators'. The IGO does, on a continual basis have one to one conversations with Co-ordinators regarding 'challenging' SARs and provides advice on the setting of parameters, redaction of third party data and application of relevant exemptions. However, as a way forward refresher training for co-ordinators is to be arranged at every other DP/FOI meeting. This will concentrate on aspects of subject access requests.

Implementation Date: June 2013
Responsibility: Indi Viknaraja

e10. The IGO maintains a central corporate subject access request log capable of recording when requests are received and responded to and the key stages in between used to record the processes undertaken. The log helps to manage requests in a timely manner, highlight when a deadline is approaching and is used to compile monthly management information on subject access performance.

e11. Every subject access request recorded on the log is linked to four correspondence folders detailing external and internal communications relevant to that request. A copy of the final response supplied to the data subject is also retained.

e12. It was noted that requests involving large volumes of personal data are handled in tranches and that data subjects are kept appraised when the deadline for their response is likely to be exceeded.

e13. The council is currently working on a proposal to transfer the logging of subject access requests to the Covalent system, which is already being utilised to log and track FOI requests. It was understood during the audit that Covalent would provide a consistent approach to the logging and tracking of requests for information at the Council. It was also noted that Covalent has advantageous features that could be used to improve subject access compliance, for example; Covalent can be configured to send automatic emails when a deadline is approaching. The ICO recognised the benefits that could be obtained from this change and would encourage the council to progress with the project.

e14. It was explained that monthly subject access compliance figures are generated by the IGO and reported upwards to the SIRO. It was also explained that this statistical information is cascaded to DP-Coordinators who analyse 'lessons learned' to help improve compliance. In addition, monthly Performance Reports are issued by directorate that incorporate subject access performance and are shared with the DMT.

e15. A SIRO report was produced in June 2012 containing statistical information relating to subject access performance. It is the intention of the Information Governance Team to produce and distribute a SIRO report on an annual basis.

e16. The DP Co-ordinator's assume responsibility for making redactions to personal data they collate from their service area for the purpose of responding to subject access requests.

e17. **It was noted that there is some variation across service areas in the way that quality checks and redactions are made and the way redaction reasons are communicated to the IGO by DP Co-ordinators. For example; some DP Co-ordinators reported they quality check their own work, others** reported a secondary **review by a peer to ensure** that **only exempt** data **is removed and others reported a quality check by the IGO. Furthermore some DP Co-ordinators explained that they complete a redaction log and others** explained **that they only discuss redactions** verbally **with the IGO.**

Recommendation: Implement a consistent approach to communicating and recording the reasons for redaction between the DP-Co-ordinators and the IGO. Reasons should be recorded **so that the council can** explain **decisions in** relation **to redactions if challenged** by **the data subject or the ICO.**
Management Response: To ensure consistency **a standard** template **that is** currently **used by C&L is to be circulated to all** co-ordinators. **This is to be completed with each case. As this can become a disproportionately time consuming and resource intensive exercise, a summary of redactions is to be maintained. This process will** also **be built into the procedures for SARs which is** used **by the DP Co-ordinators'.**

Implementation Date: June 2013
Responsibility: Indi Viknaraja

e18. The council retains both an un-redacted and a redacted version of documents issued to data subjects in response to their request. This helps to provide a complete audit trail in relation to each request and is good practice.

e19. The DP-Co-ordinators support the IGO by making initial decisions about the application of exemptions to personal data. However, the IGO makes the final decision in relation to the application of exemptions to personal data intended for release.

e20. The reasons behind the application of specific exemptions, for example; section 35 (2) are recorded in the notes column of the subject access log by the IGO.

e21. Interviewees demonstrated a good awareness of the circumstances in which the miscellaneous exemptions would apply. Awareness of the third party personal data exemption and its application in relation to subject access responses was also evident.

e22. The council has produced specific guidance for employees to follow on handling requests for personal data under section 29 of the DPA. Revenues and Benefits staff were able to describe the practical application of this guidance in their service area, including the maintenance of a section 29 log.

e23. The Principle 6 Subject Access Request Procedure outlines that final decisions on the disclosure of personal data are made by the Information Governance Team.

e24. There was evidence that requests for the disclosure of CCTV footage are forwarded to the IGO for consideration before any images containing personal data are released.

e25. Interviewees demonstrated an awareness of how to handle ad-hoc disclosure requests. It was reported that the identity of the requester, the proportionality of the request and whether consent could be obtained would all be considered prior to any disclosure being made. In addition, staff operating the Customer Service Helpdesk showed awareness of the risk posed by the unlawful verbal disclosure of personal data and use a caller identity verification process to help mitigate this risk.

e26. At interview there was inconsistency between the methodology found in the Subject Access Request Procedure and how records of disclosures are actually approved and recorded in service areas.

Recommendation: Ensure all staff understand and adhere to the disclosure process outlined in the 'Principle 6 Subject Access Request Procedure'. Ad-hoc disclosures should be signed-off by a senior member of the Information Governance Team before they take place and a central record of every disclosure retained.
Management Response: The policy will be circulated and all DP Co-ordinators' reminded of the disclosure process. The existing policy will be reviewed to ensure there are clear mechanisms in place regarding disclosures, relevant sign off and the maintenance of records. For example s29 disclosures, SARs and ad hoc (business as usual requests). At the next DP/FOI meeting this will be raised as an agenda item.

Implementation Date: August 2013
Responsibility: Indi Viknaraja

e27. The council has an established policy for data sharing with requirements based on the Essex Trust Charter standard.

e28. The council has adopted a multi-level approach with overarching data sharing agreements covering general principles agreed and signed off at senior management level, supported by subsequent agreements covering detailed or local requirements.

e29. The council's web site references a proposal to publish all data sharing agreements. It was reported that this work is under way with intention to publish on the Essex Trust Charter web site.

e30. Data sharing agreements are covered by training requirements for council staff.

e31. The Information Governance Team review data sharing agreements and are responsible for quality assurance checks.

e32. Requirements checked include the security standards applied to transfers including the use of Proofpoint for data encryption if data is emailed to a non-GSI or non NHSmail mailbox.

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

7.5 Any queries regarding this report should be directed to Aideen Oakes, ICO Good Practice Team.

7.6 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 members were particularly helpful in organising the audit – Jackie Groom (Group Manager Information and Governance) and Indi Viknaraja (Information Governance Officer).

Appendix A

Detailed findings and action plan

Action plan and progress

Recommendation	Agreed action, date and owner	Progress at 3 months	Progress at 6 months
C5. Ensure Heads of Service are aware of their responsibilities as IAO i.e. that they understand what information is held in their service, how it is used and transferred, and who has access to it and why. This could be achieved by including IAO responsibilities into relevant job descriptions and providing specific IAO role based training on an	The Council will revise the Terms of Reference of the Overarching Information Management Strategy to include IAO, Caldicott Guardian and SIRO duties. Job descriptions for Heads of Services will be revised to include their IAO and DP responsibilities. One Senior Leadership Team Meeting each year will cover a session on the roles and responsibilities of IAOs. Implementation Date: Nov 2013 Responsibility: SIRO		

	annual basis. Please see '*Local Public Service Data Handling Guidelines, version 2, August 2012'.*	
C9.	Adopt the government protective marking scheme or equivalent in all directorates. Monitor the scheme's implementation and use.	At present the Council does apply a marking system to all Reports to Council and Committees. We will now consider whether the Government Protective Marking Scheme (GPMS) can be introduced, either wholly or partly and will also consider the practicalities around the implementation. In addition, as the Cabinet Office is currently conducting a review of the GPMS to simplify it to three tiers (Official, Classified and Top Secret) the Council will continue to closely monitor how this new initiative unfolds as this will have an impact on any proposed implementation. Implementation Date: Dec 2014 Responsibility: SIRO

C10.	All staff with records management responsibilities should complete level 1 HMG Cabinet Office Protecting Information e-learning module or equivalent as part of their mandatory training. The SIRO should register with the National Archives and subscribe to the monthly SIRO newsletter. The SIRO and IAOs should consider completion of HMG Cabinet Office Protecting Information Training levels 2 and 3.	Whilst the SIRO has not completed HMG Cabinet Office Protecting Information Training, it should, however, be noted, that the SIRO has over 15 years of experience working in information governance and was responsible for setting up the first Social Care and Health information sharing protocols in the London Borough of Tower Hamlets, that went on to form the base of wider London agreements. The SIRO has been registered with the National Archives and subscription has been arranged for the monthly newsletter. As noted by the auditors the Council has an extensive training programme dealing with DP. The training programme scheduled for the coming year will have a focus on Records Management. Implementation Date: Dec 2013 Responsibility: SIRO

C11.	Select a practical deadline for all staff handling personal data as part of their job role to complete the mandatory online 'spark' data protection e-learning module. Completion of the module should be monitored and evidenced by service area.	A completion timeline of August 2013 has been agreed. Implementation Date: Aug 2013 Responsibility: Indi Viknaraja
C21.	It is recommended that the council review this part of the recall process. Consider both the secure storage of the recalled archive box once it has been retrieved by the service area that requested it and how to ensure the accuracy of both the archive log	Data transfer sheets are kept and stored electronically in Civica. Responsibility for changes that take place within the recalled boxes remain with the service areas. An updated data transfer sheet must be supplied by the service prior to the recalled box being returned to the site. Accordingly procedures have been amended and staff reminded of their responsibilities. Implementation Date: March

	and data transfer sheet.	2013 Responsibility: Karen Wright
C23.	Implement a process to ensure that only essential information is recorded by social workers in notebooks and paper assessments when offsite, and require staff to obtain manager authorisation if they want to take sensitive information offsite for other purposes.	Much of the social work activity is recorded directly into Carefirst. With the increased use of tablets/laptops the risk of transporting paper documents is reduced. As more social workers move to mobile working additional guidance and support will be given to ensure best practice continues in keeping personal data confidential and secure. Where it is necessary to take personal data off site, this will be done in line with the Council's procedures, which includes carrying them in lockable cases. Implementation Date: April 2013 Responsibility: Catherine Cobb/Ed Spacey
C28.	Create an information asset register for	In significant areas of the Council, example Revs and Bens and HR/Payroll all information is held

	physical assets storing personal data. Allocate responsibility for maintenance of physical information assets to the relevant IAOs. All information assets should be updated, reviewed and risk assessed on a periodic basis.	electronically and as such there is no requirement for an asset register. The IGO will hold a corporate physical assets register which will be reviewed annually. Implementation Date: Dec 2013 Responsibility: All areas/IGO
C30.	Produce a visitor policy for Facilities and other staff to follow, outlining their obligations and responsibilities in relation to external visitors.	The Council has an existing Security Policy which includes procedures (as listed below) which must be followed with regards to the visitors to the Civic Centre. All Members and staff are issued with identity cards that must be worn visibly at all times. Members and staff are advised to remain vigilant at all times. Members and staff are encouraged to politely challenge unscheduled visitors and suspicious situations within and around

		the premises. A visitor's register is kept at the CSC reception and visitors are issued with a visitor's badge which must be worn at all times and returned upon departure. Staff are informed when visitors have arrived and it is their responsibility to collect the visitor from reception, escort to their destination and return to reception. Implementation Date: Complete Responsibility: Karen Wright
C35.	Install lockable wall mounted key safes in service areas processing personal data, so that cabinet and pedestal keys can be securely stored in the same location. Allowing employees to take locker keys home overnight poses a	There are key safes already in place in most service areas, to include Revs and Bens, HR, various teams in ACS and Finance, Legal and Democratic Services and C&L. In areas where key safes are required they will be put in place. As a part of the ICO Audit feedback all staff have been reminded that Council papers should not be stored in personal lockers.

	data security risk, particularly if lockers are used to store personal data and so the Council should instruct employees to store locker keys in key safes overnight.	Implementation Date: June 2013 Responsibility: Karen Wright/Indi Viknaraja
C39.	It is recommended that the council implement and complete a project plan to deliver archiving and deletion solutions for both Northgate and Carefirst to ensure future adherence to retention schedules.	In Nov 2012, ACS agreed that all relevant records on Carefirst, as defined by the document retention policy would be locked down and in following 12 months deleted. A number of technical issues have caused a delay in the implementation, but it is anticipated that it will be resolved shortly and the review of the deletion process will then be initiated. The archiving solution within Northgate risks corrupting the entire database. So as things are currently, we will not be looking to implement archiving within Northgate. If and when Northgate can alter their system to

		facilitate archiving, the Council will look to implement. Implementation Date: July 2013 (for Carefirst) Responsibility: Christine Lynch, Veronica Dewsbury (Northgate) Catherine Cobb , Ed Spacey (Carefirst)
C41.	Collate and review monthly reports in relation to archiving and destruction, to help avoid retention and destruction errors. Include records management related key performance indicators in the monthly Support Services Performance Report and future annual SIRO reports.	With electronic records the new system will include retention and destruction and the ability to report. With regards to the existing system there are some limitations, example with Carefirst we are working around. With regards to hard copy records, the Council undertook a major exercise to destroy requisite files as a part of the refurbishment. This provides a good base for moving forward. Where records are stored off-site the Council will, in future, provide quarterly reports to show proper destruction of files. This will be reported as a

		part of the Support Services Performance Indicator regime. Implementation Date: March 2013 Responsibility: Karen Wright, Catherine Cobb, Indi Viknaraja
D12.	The Information Security Policy should apply to all systems and applications used to process personal data.	The Corporate Information Security Policy does cover all systems and all users – an extract below may assist. The fact that administration of some systems such as Carefirst are managed at business level does not mean that they do not comply with the Policy. Those who are granted access to Information and information systems must: Only access systems and information, including reports and paper documents to which they are authorised. Use systems and information only for the purposes for which they

have been authorised.

Comply with all applicable legislation and regulations.

Comply with the controls defined by the Information Asset Owner.

Comply with all Southend-on-Sea Borough Council Policies, Standards, Procedures and Guidelines, along with the policies and requirements of other organisations when granted access to their information.

Not disclose confidential or sensitive information to anyone without the permission of the Information Asset Owner, and ensure that sensitive information is protected from view by unauthorised individuals (eg. public places).

Keep their passwords secure, not allowing anyone else to use their account to gain access to any system

or information.

Protect information from unauthorised access, disclosure, modification, destruction or interference.

Not attempt to disable or bypass any security features which have been implemented.

Notify your Line Manager of any actual or suspected breach of Information Security, or of any perceived weakness in the organisation's Security Policies, Procedures, Practices, Process or Infrastructure in accordance with the Data Security Breach Procedure.

Implementation Date:
Complete
Responsibility: Kim Karacolak

We have been auditing mobile devices such as laptops and will be updating our IT asset register.

	Implementation Date: August 2013 Responsibility: Kim Karacolak
D15. Implement procedures to ensure regular and accurate updating of the IT asset register.	The Council plans to introduce methodology and technology to only allow registered and encrypted removable media. This will be introduced through a staged process that will allow measures to be put in place over an agreed period of time to ensure minimal operational impact to the business.
D16. The council should consider implementing a memory device 'amnesty' so as to collect any redundant media in line with policies adopted by other local authorities when implementing endpoint control systems.	Implementation Date: Nov 2013 Responsibility: Kim Karacolak
D29. Additional security	Installing turnstiles will now form part of the new ground floor layout to be implemented in the next phase of the Civic Centre refurbishment. For additional security the Council is also considering changing CCTV for improved images and restricting access to points of access during out of office hours.

	should be provided reflecting the approach of other councils with similar civic centres. Options include installing turnstiles at the lobby entrance.	Implementation Date: March 2014 Responsibility: Martin Musgrave/Karen Wright Rejected - the printers work on the basis of 'print and delete'. In addition, the data is automatically deleted on a pre-set time line e.g. 24 hours. For equipment that is taken away e.g. MFD's these are either wiped or destroyed, dependant upon whether the equipment is to be recycled
D31.	MFDs should be treated as PCs in terms of security policies with disks over written if leaving council premises in line with the IT Media Policy.	Implementation Date: Rejected Responsibility: This will be implemented immediately. Implementation Date: Feb 2013 Responsibility: Kim Karacolak

D34.	Requests for temporary / contract staff should include the contract duration so that this can be included in the network account set-up with duration time included in the Active Directory setting. A default time duration reflecting minimum contract times should be used if no time is defined by requesting managers.	A leavers checklist for manage is produced by HR. This is a form managers complete and send to HR when an employee leaves. Although this is for HI purposes it will be amended t remind managers that they must ensure ICT and facilities are advised to cancel their access to ICT systems and the ID card within a prescribed tir It will also impress that for managers who fail to do so it will be logged as a security incident which will be reporte to the SIRO. Implementation Date: August 2013 Responsibility: Kim Karacolak, Sue Putt
D35.	Any failure by line managers to notify IT of staff leavers should be treated as a security incident and reported to the Information Governance Team.	

	Endpoint controls are to be introduced by the end of March. Implementation Date: March 2013 Responsibility: Kim Karacolak
D40. The introduction of endpoint controls should be treated as a security priority. Until then additional awareness campaigns will be required to reduce risks.	The Council will have another test carried out by the end of this year. Implementation Date: Dec 2013 Responsibility: Kim Karacolak
D47. Social Engineering penetration tests should cover high risk areas such as the Customer Service Centre Helpdesk.	The PIA process is covered in the Project Management Guidance which has already been commissioned. This is a 2 part document which comprises the detailed guidance and the Quick User Guide. Sign off and roll out to be carried out before June.

E17. Implement a consistent approach to communicating and recording the reasons for redaction between the DP-Co-ordinators and the IGO. Reasons should be recorded so that the council can explain decisions in relation to redactions if challenged by the data subject or the ICO.	To ensure consistency a standard template that is currently used by C&L is to be circulated to all co-ordinators. This is to be completed with each case. As this can become a disproportionately time consuming and resource intensive exercise, a summary of redactions is to be maintained. This process will also be built into the procedures for SARs which is used by the DP Co-ordinators'. Implementation Date: June 2013 Responsibility: Indi Viknaraja The policy will be circulated and all DP Co-ordinators' reminded of the disclosure process. The existing policy will be reviewed to ensure there are clear mechanisms in place regarding disclosures, relevant sign off and the maintenance of

E26. Ensure all staff understand and adhere to the disclosure process outlined in the 'Principle 6 Subject Access Request Procedure'. Ad-hoc disclosures should be signed-off by a senior member of the Information Governance Team before they take place and a central record of every disclosure retained.		records. For example s29 disclosures, SARs and ad hoc (business as usual requests). At the next DP/FOI meeting this will be raised as an agenda item. Implementation Date: August 2013 Responsibility: Indi Viknaraja