Audit Committee
Tuesday 18 June 2013
Item No. 11

MIDLOTHIAN AUDIT SERVICES
INTERNAL AUDIT REPORT

Subject:	Follow up Review - Data Protection
Issued to:	John Blair, Director, Corporate Resources Don Ledingham, Director, Education and Children's Services Eibhlin McHugh, Acting Director, Communities and Wellbeing Heads of Service Philip Timoney, Business Service Manager Ian Pilbeam, Corporate HR Strategy Manager Iain Johnston, Procurement Manager Ian Wragg, Information Security Officer Magnus Inglis, Performance and Planning (Divisional IMG Chair) Rebecca Fairnie, Performance and Information Systems Manager Acting Up (Divisional IMG Chair) Other IMG & DIMG members (via Philip Timoney)
Copied to:	Gary Fairley, Head of Finance and Human Resources (s95 officer) Other Members of the Corporate Management Team
Submitted to:	Audit Committee – June 2013
Date:	5 June 2013

Author: **Graham Herbert, Internal Audit** **ext 3517**

EXECUTIVE SUMMARY

Objective of the Audit

The objective of the audit was to review progress towards implementing the agreed Management Action Plan following the Internal Audit review of Data Protection which was completed in November 2011 and to consolidate any remaining issues with those raised by the Information Commissioner into a single action plan.

Scope of the Audit

The audit focussed on:

- the adequacy of actions taken by management on any issues raised that have been flagged as closed on Covalent (the Council's Performance Management System);
- an assessment of the number and materiality of any issues that remain open; and
- integrating issues raised by Internal Audit and the Information Commissioner into a single action plan.

Excluded from Scope

This was not a full audit of Data Protection with testing undertaken limited to confirm that actions have been closed as per the agreed management action plan.

Follow-up Audit

As is standard practice for Internal Audit, we have not rated this review since it is a follow-up of a previous Audit. We have however raised recommendations where we have agreed with management that further improvements can be made and note that the Information Commissioner ranked Midlothian Council as having "Reasonable Assurance" (please see the Audit Opinion for more details on the rating scales).

Background

In 2011, Internal Audit undertook a review of Data Protection within the Council and rated the review as Amber. A total of 36 management actions were raised with agreed implementation dates ranging from January 2012 to June 2012.

The scope for the original audit covered the following areas:

- data protection governance, for example polices and procedures, codes of practice and training;
- the Council's data protection notification;
- compliance with individual's rights, such as subject access;
- mechanisms for ensuring that personal data is obtained and processed fairly, lawfully and on a proper basis (including the use of fair processing notices);
- processes for ensuring personal data is accurate, complete, up to date, adequate, relevant and not excessive;
- procedures for review, deletion and retention of personal data;
- the procedures adopted for sharing and disclosing personal data; and

- the secure processing of personal data.

The Council was fined £140K by the Information Commissioner in January 2012 for disclosing sensitive personal data relating to children to the wrong recipients on five separate occasions. This was reviewed by the Data Protection Breach Team and actions implemented to improve controls going forward.

The Information Commissioner was invited to undertake a review of compliance with the Data Protection Act in March 2013 because of this fine and their conclusions and recommendations are included in this consolidated report.

Conclusions

The Information Commissioner's Office ranks those it audits on the following scale:

- high assurance;
- reasonable assurance;
- limited assurance; and
- very limited assurance.

Midlothian Council was awarded a rating of "Reasonable Assurance". The explanatory note that accompanies this award is:

"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". The ICO noted areas for improvement and made 28 recommendations.

Internal Audit's follow up identified that some issues raised in the 2011 report had been addressed (8). Others had been partially implemented (13) while (15) remained outstanding.

Both the ICO and Internal Audit recommendations that remain outstanding have been consolidated into a single action plan to track progress in implementing the agreed issues and these are detailed in Appendix 1 of this report.

Appendix 2 is a copy of the Information Commissioner's Report.

APPENDIX 1 – COMBINED ACTION PLAN ENCORPORATING INFORMATION COMMISSIONER'S OFFICE RECOMMENDATIONS AND ISSUES THAT REMAINED OUTSTANDING FROM INTERNAL AUDIT'S 2011 REPORT

Rec No	Recommendation	Management Comment Priority	Priority	Responsibility	Target Date
1	A terms of Reference needs to be developed for the Central Information Management Group (CIMG) and the Divisional Information Management Groups (DIMG). This should include: composition; frequency of meetings; requirement to attend or send a deputy; reporting lines (e.g. CMT, DMT and CIMG); and frequency of reporting progress against the action plan.	Agreed.	Medium	IMG / DIMG	30/09/13
2	The composition of the DIMG should be regularly reviewed and be a regular agenda item with any missing representation addressed (for example in Communities and Wellbeing inclusion of a Day Services Officer and in Corporate representation from Council Secretariat).	Agreed.	Medium	DIMG	31/08/13 Annually thereafter.
3	Policies and procedures should all be reviewed annually, unless otherwise stipulated. Midlothian Council should arrange for the review process to be monitored to help mitigate the risk of policies not being routinely reviewed and therefore potentially containing inaccurate information.	Agreed. Polices and procedures will be reviewed annually. This will be added to the IMG / DIMG plan.	Medium	IMG	30/04/14
4	Risk assessments for data protection risks should be reviewed on a regular basis; detail controls and specifically address any high risk areas. In order to facilitate this DIMG chairs should be given view / update authority for relevant risks.	Agreed.	Medium	Heads of Service / DIMG	31/08/13 Quarterly thereafter.

5	The Council's Authorised Signatories database should be populated with those who have authority to authorise user access to IT systems.	Agreed.	Medium	DIMG	30/04/14
6	When rolling out the Metacompliance software consider incorporating a mechanism to ensure that data protection related policies are communicated to all new and existing staff including agency workers and contractors and that acceptance by staff is captured by the system.	Agreed.	Medium	IMG	30/04/14
7	Ensure that the Senior Information Risk Officer's (SIRO) remit includes a formal requirement to routinely report to the Corporate Management Team on compliance with the DPA.	Agreed – SIRO's remit to be amended and published on the Intranet along with other Information Management Group remits.	Medium	IMG / Head of Customer Services	31/08/13
8	Ensure data protection responsibilities are reflected in work related objectives / competencies of all relevant staff (including the SIRO). Internal Audit had previously recommended that generic competencies need to be developed for CIMG and DIMG representatives through development of work related objectives. These could include expectations for regular and active attendance at CIMG and DIMG meetings.	Consultation will be scheduled between the SIRO, IMG Chair and HR Services as to the best approach to achieve this.	High	SIRO and IMG Chair.	30/06/13
9	Provide specialised DPA training where there are key roles in relation to Information Governance. Internal Audit had previously identified that a formal training strategy needed to be developed.	Agreed. Training providers will be identified for all key staff with DPA responsibilities and included in the training strategy which is under development.	High	IMG	31/10/13

10	Finalise the Information Asset Register and introduce a robust method of routinely monitoring and updating it. (This had been noted as outstanding from the previous Internal Audit review).	Agreed. SMART objectives will be added to IMG action plan 2013-15.	High	IMG	30/04/14
11	Implement a formal reporting mechanism to ensure the SIRO provides the Accounting Officer (Chief Executive) with written advice, at least annually, to inform the annual governance statement. The advice should draw on support evidence provided by the Information Assurance Officers (IAOs) and other specialist roles.	Agreed. Internal Audit and SIRO will provide written advice annually to inform the governance statement.	Medium	SIRO	30/04/13 Annually thereafter.
12	Implement a series of KPIs to give the IMG oversight of compliance by MC regarding areas of risk. Internal Audit previously recommended that DIMG should undertake regular reviews of: • local procedures; • privacy statements; • the need to undertake regular physical security audits; • regular quality checking of data held and compliance with retention policy; and • monitor the level of compliance over new starts undertaking MILO training within three months of starting.	Agreed.	High	IMG	31/05/13
13	Privacy impact assessments (PIAs) should be carried out for all significant projects and involve data protection considerations. MC should add this recommendation to the IMG Action Plan so progress can be regularly assessed.	IMG action plan will be updated so that progress can be assessed on a quarterly basis.	Medium	IMG	30/04/14

14	On line privacy statements should be reviewed to ensure that they are compliant with the standard Council statement and the ICO guides and be made more visible to those completing the forms.	Agreed.	Medium	IMG / DIMG	30/04/14
15	Corporate DIMG should review privacy statements recorded on hard copy forms to ensure compliance with the standard Council statement and the ICO guides (Communities and Wellbeing and Education and Children's Services still have this issue open on Covalent).	Agreed.	Medium	IMG/DIMG	31/12/13 Annually thereafter
16	Current guides on the use and format of privacy statements needs to be expanded to include: • how the privacy statement should be used; • to place the statement above any signature box; • to use plain English; • provide contact opt outs for certain types of information (e.g. email contact); and • providing Council contact details should further details be required.	Agreed.	Medium	IMG / DIMG	30/04/14
17	Develop refresher training in relation to data protection and security of personal data. Internal Audit had previously identified that a formal training strategy needed to be developed.	Agreed. This has been added to the IMG 2012-15 action plan.	Medium	IMG	30/03/13
18	Introduce regular monitoring of new members of staff who have not completed their MILO training within the required three month period with clear escalation where this has not been achieved.	Agreed.	High	Corporate HR Strategy Manager / DIMG	31/05/13

19	Provide figures for review and sign off to the SIRO and the IMG in relation to attendance for the courses made available for staff on data protection and information governance.	Agreed. A report will be submitted to IMG as a standard reporting item.	Medium	IMG	31/07/13 Half yearly thereafter.
20	Update contract logs to highlight contracts which involve personal data. (This had been noted as outstanding from the previous Internal Audit review).	A new Midlothian Council Contract Register has recently been developed and a further field will be added that will highlight any contracts that have personal data.	High	Procurement Manager	30/05/13
21	Implement contract management guidance for all areas of the Council. Where there are areas of good practice already in place (for example Social Work) these can be drawn for the process.	Agreed. Contract and Supplier Management Guidance has been written but still remains in draft format. Enhanced monitoring / annual assurance checks to be added to guidance. The Scottish Government is currently developing a contract supplier management module which will be part of the Public Contracts Scotland portal. All supplier meetings / contract compliance checks throughout the contract duration will be uploaded to this system.	Medium	Procurement Manager	30/06/13 (roll out of Contract and Supplier Management guidance). Scottish Government Module will be adopted after pilot is complete.
22	Provide secure storage for areas where personal data is processed manually so that they can be locked away at night. (Internal Audit had previously identified the need to undertake clear desk policy checks).	Agreed. Secure file storage has been identified as part of Effective Working in Midlothian project. Individuals and teams will have access to new lockable cabinets.	High	IMG	31/10/14
23	Implement monitoring and reporting on the clear desk policy. (Internal Audit had previously identified the need to undertake clear desk policy checks).	Agreed. Staff to be reminded of clear desk policy (via Metacompliance). Random compliance checks to be carried out by Line managers and DIMG members.	Medium	DIMG / Line Managers	31/10/14

24	Minimise the access to fax machines to prevent any accidental disclosures, and implement the proposed secure printing measures.	Agreed. The implementation of new multi-function devices will reduce the need for fax machines. These devices (MFDs) will not print until recipient inputs a user code. The Council is looking to reduce the number of fax machines in operation and move to more secure technologies over time.	Medium	Procurement Manager / Commercial Services Manager	30/06/14
25	Ensure that where even unsuccessful attempts to transfer data take place they are highlighted and investigated.	Rejected. The Council has introduced software designed to explicitly prevent data transfer to unauthorized USB devises. The product is CESG CCTM approved and deemed fit for purpose. The resource required to identify and then investigate unsuccessful attempts outweighs the benefit. Limited security resource would be better used elsewhere as agreed during the audit.	N/A	Information Security Officer.	N/A
26	Consider disabling access to hard drives in desk top machines.	Agreed. The Council will consider disabling access to hard drives as part of the PC desktop replacement program, although it is highly unlikely that it could ever be universally applied.	Medium	Information Security Officer.	30/03/14
27	Develop KPIs for systems to provide the SIRO / IMG with reporting to allow high level oversight of systems (e.g. Frameworki).	Agreed	Medium	IMG	31/07/13
28	Hard copy subject access request (SAR) forms need to be made available at Council offices	Agreed.	Medium	IMG / DIMG	30/03/14

29	Subject access guidance on the Council Intranet needs to be expanded to include: • identify the subject access officers in each Division; • require the quality assurance checks on responses; • provide training through introduction of a MILO course or use of Metacompliance; and • Information of when a referral to Legal is required (e.g. concern over an individual's identity or over the information requested).	Agreed.	Medium	IMG	30/03/14
30	Consider refining the existing SAR process so that there is more central oversight (for example centralising quality assurance). This will also enable a knowledge bank of best practice to be built up for reference by the service areas that may only infrequently come across SARs.	Agreed. The SAR process is currently under review and recommendations will be integrated into the new procedure. Nominated officers for each division have been identified to monitor SARs.	Medium	IMG	31/01/14
31	Formally document responsibilities in competency framework for processing SARs. Internal Audit had previously recommended that generic competencies need to be developed for CIMG and DIMG representatives through development of work related objectives.	Agreed. Role descriptions will be created for staff responsible for processing SARs	Medium	IMG	31/01/14

32	Implement awareness training for staff on how to recognise if a SAR is being made, consider building on MC’s existing freedom of information training modules (how to recognise a freedom of information request) to achieve this. Internal Audit had previously identified that a formal training strategy needed to be developed.	An E-learning module will be created and training sessions conducted to increase awareness.	Medium	IMG	31/01/14
33	Consider clarifying the process regarding dealing with SARs that involve cross divisional searches to ensure they are logged and processed correctly, in a timely manner, and that MC staff know who to pass them to (perhaps a central resource such as the Data Custodian). Internal Audit previously recommended that long term, a Council-wide tracking and administrative system should be developed to provide consistency over the process as is the case for Freedom Of Information requests	SAR process currently under review. Role and responsibilities will be clearly defined. A template has been developed outlining search and timescales to respond.	Medium	IMG	31/01/ 14
34	Ensure that key staff responsible for dealing with SARs, disclosures, redactions, exemptions and data sharing receive appropriate training and on-going periodic refresher training which is logged centrally and monitored. Internal Audit had previously identified that a formal training strategy needed to be developed.	Key staff will be trained in dealing with the more specialised aspects of the DPA especially SARs and data sharing.	Medium	IMG	30/03/14

35	Update procedure to include exemptions to DPA 98 (when information does not need to be reported to a data subject on request), how to apply them and suitable review process to ensure they have been correctly applied.	The SAR review process is currently being reviewed. Revisions will include guidance on the application of exemptions.	Medium	IMG	30/03/14
36	Introduce a method of quality assuring responses to SARs such as dip sampling of a selection of responses by line managers to ensure that exemptions are being considered and applied correctly. Internal Audit had previously identified the need to introduce checking routines.	Midlothian Council will sample 10% of SARs and third party sharing agreements to ensure quality and consistency of response.	Medium	IMG	30/03/14
37	Introduce a consistent process for considering and responding to requests for personal data; both third parties and SARs. Include a requirement to record responses and partial responses given by MC to provide an audit trail. Include details in the records that demonstrate decisions disclosing or withholding information. Internal Audit had previously recommended consistency of reporting over SARs.	Sharing agreement documentation suite to be developed along with SAR process review, placing a greater emphasis on recording of actions etc.	Medium	IMG	30/03/14

Appendix 2- Information Commissioners Report

Midlothian Council

Data protection audit report

Information Commissioner's Office

Auditors:	**Claire Chadwick - Team Manager (Audit)** **Paul Hamnett – Engagement Lead Auditor** **Carol Knights – Lead Auditor**
Data controller contacts:	**Hillary Kelly – Head of Customer Services & SIRO**
Distribution:	**Kenneth Lawrie – Chief Executive**
Date of first draft:	22 March 2013
Date of second draft:	10 April 2013
Date of final draft:	2 May 2013
Date issued:	**2 May 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 Midlothian 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 Midlothian Council (MC) was issued with a Civil Monetary Penalty by the ICO in January 2012 following several data security incidents. As a result MC invited the ICO to conduct a consensual audit of its processing of personal data.

1.4 An introductory teleconference call was held on 22 January 2013 with representatives of MC to identify and discuss the scope of the audit.

2. Scope of the audit

2.1 Following pre-audit discussions with MC it was agreed that the audit would be limited to the Revenues and Benefits, Travel Team and Criminal Justice areas of MC and focus on the following areas:

a. Data protection governance – The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

b. 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.

c. Requests for personal data – The processes in place to respond to any requests for personal data. This will include requests by individuals for copies of their data (subject access requests) as well as those made by third parties and sharing agreements.

3. Audit opinion

3.1 The purpose of the audit is to provide the Information Commissioner and MC with an independent assurance of the extent to which MC, 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 3 reasonable assurance assessments of scope areas where controls could be enhanced to address the issues which are summarised below and presented fully in the 'detailed findings and action plan' at section 7 of this report.

4. Summary of audit findings

4.1 Areas of good practice

- The Information Management Group run training sessions that are open to all staff. These raise awareness of issues and MC policy. There are also sessions for councillors to ensure they are aware of information governance issues.

- There was evidence of MC supplying advice to customers about how to request copies of their personal data.

- There is an IT asset register that is used to track MC equipment through the lifecycle. This includes when equipment is destroyed.

- There are formal procedures for reporting incidents that include escalating serious incidents to the Data Breach Team. Sensitive breaches involving personal data are escalated to the Information Security Officer and the Senior Information Risk Owner. There is also a log of all security incidents.

- MC has introduced a series of Baseline Security Checks when dealing with third sector organisations. These measures provide a minimum requirement that has to be met in order to provide services.

4.2 Areas for improvement

- The process of recognising and mitigating risks through an Information Asset Register has not been fully implemented. Information Asset Owners have not been assigned for all information assets and a method of continuing assessment has not been implemented.

- There were no key performance indicators used to give the Information Management Group oversight of compliance regarding areas of risk.

- There was no specialised training for staff with responsibilities for dealing with requests for personal data.

- The process for a central log of all MC data sharing agreements has not been finalised.

- Currently there are no central requirements in the corporate procurement process in relation to managing contracts. There is a log for contracts although this does not highlight areas where personal data is involved.

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 the following locations between 5 and 7 March 2013:

- Midlothian House
- Fairfield House
- Buccleuch House
- Dalkeith Social Work
- Jarnac Court
- Dundas Buildings

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

7.1 Scope: Data protection governance. The extent to which data protection responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor DPA compliance are in place and in operation throughout the organisation.

Risk: Without a robust governance process for evaluating the effectiveness of data protection policies and procedures there is a risk that personal data may not be processed in compliance with the DPA resulting in regulatory action and/or reputational damage.

a1. MC has a range of policies and procedures relating to data protection. These include a Privacy Policy, Information Security Policy and Data Sharing guidelines; they are available to all staff on the MC Intranet.

a2. Policies seen by auditors do not follow an agreed format, styling and version control process. They are produced and ratified via a number of different channels across MC including the Information Management Group (IMG) or directly produced by various services.

Recommendation: Policies and procedures should all be reviewed annually, unless otherwise stipulated. MC should arrange for the review process to be monitored to help mitigate the risk of policies not being routinely reviewed and therefore potentially containing inaccurate information.

Management response: Agreed. Policies and procedures will be reviewed annually. This will be added to the IMG action plan.

Implementation date: March 2014

Responsibility: IMG

a3. MC produces updates that inform staff of the guidance available and there is a dedicated information governance page which provides staff with a central point of call, to find advice and guidance on complying with their data protection responsibilities. This includes Top Tip documents and other useful guidance material to raise staff awareness on keeping data safe. Auditors also observed posters highlighting various data protection issues.

a4. All staff must sign the ICT Acceptable Use Policy and those using memory sticks, smartphones and laptops must also sign the corresponding policy. There is currently no requirement for staff to sign off acceptance for other policies, however, interviews established that Meta-Compliance policy management software was in use and this currently formed part of the IMG Action Plan deliverables.

Recommendation: When rolling out the Metacompliance software consider incorporating a mechanism to ensure that data protection related policies are communicated to all new and existing staff including agency workers and contractors and that acceptance by staff is captured by the system

Management response: Agreed

Implementation date: March 2014

Responsibility: IMG

a5. There is a structured governance framework in place to support the data protection and information governance management agenda.

a6. Overall responsibility for data protection has been allocated at Heads of Service level rather than Board level. However, the Senior Information Risk Officer (SIRO) also sits on MC's more senior executive forum, the Corporate Management Team (CMT) which is chaired by the Chief Executive. This is in line with the requirements of the Identity Management and Privacy Principles produced by the Scottish Government which require reporting to the "Board or equivalent". In addition the SIRO is also MC's nominated monitoring officer for the purposes of the Local Government Act.

a7. The SIRO was appointed to the role in 2011. Her general role description does not explicitly set out her SIRO responsibilities although general responsibilities are set out MC's Privacy Policy.

a8. The IMG reports to CMT via the SIRO and the SIRO takes reports on an ad hoc basis to the CMT from the IMG although this is not a standing agenda item at CMT.

Recommendation: Ensure that the SIRO's remit includes a formal requirement to routinely report to the CMT on compliance with the DPA.

Management response: Agreed – SIRO remit to be amended and published on intranet along with other IMG remits

Implementation date: Aug 2013

Responsibility: IMG & SIRO

a9. There is an Information Management Group (IMG) which is responsible for information governance and data protection compliance activity. Membership consists of representatives of all Council Heads of Service plus a range of senior information governance staff such as a data custodian, the MC solicitor and the IT Security Officer. The IMG has an Action Plan in place by which the IMG routinely monitors and mandates data protection matters, including governance, security, and records management.

a10. There are Divisional IMGs (DIMGs) in place for each area of MC which routinely report up to the main IMG.

a11. Data protection roles and responsibilities are not routinely included in job or role descriptions. Some relevant responsibilities are referred to in staff appraisals in the form of work objectives or general behavioural competencies.

Recommendation: Ensure data protection responsibilities are reflected in the job descriptions of all relevant staff (including SIRO).

Management response: Consultation will be scheduled between SIRO, IMG Chair and HR Services as to the best approach to achieve this.

Implementation date: June 2013

Responsibility: SIRO & IMG Chair

a12. Responsibility for drafting a Statement of Internal Control (SIC) has been assigned to the Audit and Risk Manager. The current SIC contains reference to data protection issues. This is not mandatory, it would be good practice to formalise the process for preparing the SIC to include appropriate input regarding data protection

a13. The SIRO has not taken the specialised training for the role that is offered by The National Archive. Although IAOs have not all been fully appointed, those that were in place have not had any specialised training for their roles.

Recommendation: Provide specialised training where there are key roles in relation to Information Governance are identified

Management response: Agreed. Training providers will be identified for key staff with DPA responsibilities.

Implementation date: Oct 2013

Responsibility: IMG

a14. MC has a risk management framework in place. There is a Risk Management Group (RMG) which is chaired by the Risk and Audit Manager, with the Information Security Officer in attendance. This looks at the high level corporate risks and more detailed departmental level risks. Both these include information risks. MC is aware that terms of reference for the RMG are required to be updated as they do not refer to the IMG.

a15. MC produces a detailed framework of risk registers ranging from high level corporate risks to more detailed departmental level risk registers. Information risks are considered at each level, for example "governance" as a risk is allocated to the SIRO in the high level corporate register and risks relating to the need for regular review of security policies are dealt with in the information security risk register. The risks are routinely reviewed at the appropriate forums. For example, corporate level risks are reviewed quarterly by the CMT.

a16. MC's risk management activity feeds into the overarching cycle of audit planning and assurance observed to be in place within MC. Recent audit activity has included a data protection audit.

a17. Although MC has a log of software and assets in place, they are currently in the process of producing a more comprehensive Information Asset Register (IAR) with business critical assets being logged as a priority area. IAOs either have been allocated to all information assets, or will be once the IAR is complete. When complete, this will ensure that MC has assurance that their information assets are logged and that inward and outward data flows have been identified.

Recommendation: Finalise the IAR and introduce a robust method of routinely monitoring and updating it.

Management response: Agreed. SMART objectives will be added to IMG action plan 2013-15
Implementation date: March 2014

Responsibility: IMG

a18. We established in interview that the Chief Executive was the MC Accounting Officer, although it is unclear if this was formally documented. We were unable to establish if the SIRO provided the Chief Executive / Accounting Officer with written assurances that information risks are being assessed and mitigated to an acceptable level and likewise if the IAOs provided the SIRO with similar written assurance.

Recommendation: Implement a formal reporting mechanism to ensure the SIRO provides the Accounting Officer with written advice, at least annually, to inform the annual governance statement. The advice should draw on supporting evidence provided by the IAOs and other specialist roles.

Management response: Agreed. Internal audit & SIRO will provide written advice annually to inform governance statement.

Implementation date: March 2014

Responsibility: SIRO

a19. There is an internal audit function which conducts regular audits throughout MC. These were observed to include data protection related audits which are currently being followed up this audit year. The outstanding actions from the last data protection audit form part of the IMG Action Plan deliverables.

a20. While no detailed data protection key performance indicators were observed to be currently produced for MC it was noted that this was something that was listed as a future deliverable on the IMG Action Plan.

a21. The Action Plan functions as a central plan for data protection, information governance, records management and information security measures being implemented. It regularly measures progress against targets and provides the IMG with a general overview of performance against achievement of key deliverables such as completion of the IAR and development of a performance matrix.

a22. Although progress against the Action Plan is reported to the IMG, there is no comprehensive management information routinely escalated to the CMT demonstrating data protection compliance.

Recommendation: Implement a series of KPI's to give the IMG oversight of compliance by MC regarding areas of risk.

Management response: Agreed, though clarification required. Can the ICO advise as to which area's the ICO considers essential KPI's for DP risk reporting\ monitoring.

Implementation date: July 2013

Responsibility: IMG

a23. A detailed Privacy Impact Assessment (PIA) process is available on the Intranet. However, in interview it was explained that PIAs are not currently mandatory.

Recommendation: Privacy Impact Assessments (PIAs) should be carried out for all significant projects that involve data protection considerations. MC should add this recommendation to the IMG Action Plan so progress can be regularly assessed.

Management response: IMG action plan will be updated so that progress can be assessed on a quarterly basis.

Implementation date: March 2014

Responsibility: IMG

a24. One PIA has been entered into by MC. It was carried out prior to the use of biometric data in schools. The data custodian (a member of the IMG) was named as MC contact point and prepared the PIA. It includes detailed review of the applicability of the data protection principles to the project.

a25. In interview auditors established that no further PIAs had been entered into and were advised that there was currently some resistance to wider roll out.

a26. MC did not currently keep a register of PIAs due to the fact that only one had been entered into. Where there is an increase of PIAs there should be a central log kept.

7.2 Scope: 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.

b1. In addition to the IAR which is being produced, there is also an IT asset register. This includes the location and (where the hardware has been issued) owner of the hardware. It also shows the status which includes hardware that has been destroyed.

b2. MC uses Microsoft System Center Configuration Manager (SCCM) to track and monitor their hardware.

b3. There was a one off reconciliation exercise that was conducted last year as part of a rationalisation program to ensure the hardware register was up to date.

b4. There is a formal Incident Reporting Policy that requires staff to report security incidents. This includes how to define the information security incident and who to report them to.

b5. All incidents have to be reported to the line management and are escalated depending on the severity. Incidents including elements of IT are logged with the IT helpdesk. Where the incident is of a sensitive nature the ISO or SIRO should be informed.

b6. There is a form for reporting any incidents which is available electronically. The policy sets out MC's duty to review any incidents, take appropriate action, and report back on any lessons learned or changes that need to take place.

b7. All incidents will be reviewed by the Risk Management Group and serious incidents are escalated to the Data Breach Team.

b8. There were log in place (the UNIRAS database) that detailed any data breaches. MC was in the process of considering publishing data breaches on their website.

b9. There is mandatory e-learning in place on the Midlothian Interactive Learning Online (MILO) that covers security training which is available to staff on the MILO system. This has recently been completed by all staff and there is currently no refresher training in place.

Recommendation: Develop refresher training in relation to data protection and security of personal data.

Management response: Agreed. This has been added to the IMG 2013-15 action plan.

Implementation date: March 2014

Responsibility: IMG

b10. The IMG run training seminars for around 50 people at a time that cover elements of data protection and information governance. These are not mandatory, but session attendance has been monitored, and has been high. It was not established if the figures on attendance were formally reported to the SIRO or the IMG.

Recommendation: Provide figures for review and sign off to the SIRO and the IMG in relation to attendance for the sessions

Management response: Agreed. A report will be submitted to IMG as a standard reporting item.

Implementation date: July 2013

Responsibility: IMG

b11. There is a staff magazine which the ISO writes a regular column in to raise security awareness.

b12. The ISO can attend team meetings if there is an issue that they require guidance on.

b13. Meta-compliance has been rolled out to ensure staff read and confirm their understanding of policies. This forces them to read the policies and answer question to help ensure they are understood. MC is currently in the processes of updating the policy suite with mandatory policies.

b14. There are specialist applications from the different areas that we visited. Some of these had specialist training requirements that had to be completed before access was allocated.

b15. Third party contracts are set up as part of the procurement process. This includes areas where personal data is used.

b16. There are standard contract requirements in relation to data protection that are required by the Scottish Government. MC decided to implement their own that they felt offered better assurance as they detailed more specific requirements for compliance.

b17. The value of the contract dictates the type of contract used. For contracts over £5,000 procurement would be involved in the sign off process. For those that are less than £5,000 sign off would only be required from an authorised signatory. Even if procurement is not required for the sign off they still retain details of the contracts on their log.

b18. The log shows who is responsible for any contracts and records any associated risks. However, it does not highlight contracts where personal data is involved.

Recommendation: Update the log to highlight where contracts involve personal data.

Management response: A new Midlothian Contract Register has recently been developed and a further field will be added that will highlight any contracts that have personal data.

Implementation date: 30/05/2013
Responsibility: Iain Johnston

b19. Within social work there are measures in place in relation to contract management. These include checks prior to the contract being implemented and annual assurances that they are compliant.

b20. There are also Baseline Security Checks (BSC) that have been developed for use with third sector organisations that are providing services to MC. Where a third sector organisation cannot demonstrate the requirements of the BSC their bid is rejected. This is seen as good practice.

b21. However, there are no central requirements in the corporate procurement process in relation to managing contracts. They are looking at ways to implement standards across MC.

Recommendation: Implement contract management guidance for all areas of the council. Where there are areas of good practice already in place (for example social work) these can be drawn on for the process.

Management response: Agreed. Contract and Supplier Management Guidance has been written but still remains in draft format, enhanced monitoring/annual assurance checks to be added to guidance. Scottish Government currently developing a contract and supplier management module which will be part of the Public Contracts Scotland portal, all supplier meetings/contract compliance checks

throughout the contract duration will be uploaded to this system.

Implementation date: **Contract & Supplier Management Guidance will be rolled out to key/business critical contracts from June 2013, the Scottish Government Module is currently in development but early indications that it will be completed and piloted over the summer 2013, Midlothian will adopt after the pilot is complete.**

Responsibility: **Iain Johnston**

b22. Access into the buildings we visited is controlled by swipe card access. This allows zoning so that staff can only get access to areas they are supposed to be in.

b23. Access is also restricted to contracted working hours. Where out of hours is required this is applied for a set amount of time (for example, overtime on a weekend). This is considered good practice.

b24. For all MC sites there are locked confidential waste bins. These are collected by facilities and stored in a secure locked area at the head office building.

b25. An external contractor shreds the bags fortnightly onsite. They issue a destruction certificate for the paper destroyed and these logs are retained by MC.

b26. Hardware is kept in a secure locked areas by IT. All hardware capable of storing information is degaussed before being destroyed or recycled by a contractor. There are certificates of destruction supplied and the log is updated to reflect the status of the hardware.

b27. There is a clear desk policy (CDP) in place and the staff that we interviewed were all aware of the requirements to lock material away. However, one of the areas visited (revenues cash office) were storing completed forms in boxes in their office. The office was in a secure area where a key code was required to gain access to the area.

Recommendation: **Provide secure storage for areas where personal data is process manually so they can be locked away overnight.**

Management response: **Agreed. Secure file storage has been identified as part of Effective Working in Midlothian (EWIM) project. Individuals and teams will have access to new lockable cabinets**

Implementation date: **Oct 2014**

Responsibility: IMG

b28. There is no monitoring of the CDP in place, such as sweeps by the last person to leave an area to ensure no material is left out.

Recommendation: Implement monitoring and reporting of the CDP.

Management response: **Agreed. Staff to be reminded of CDP policy (via Metacompliance). Random compliance checks to be carried out by Line managers and IMG members.**

Implementation date: **Oct 2014**

Responsibility:

b29. There is a procedure in place for the secure use of fax machines. All of the staff that we interviewed said that faxes were seldom used for sending material and were there more for receiving documents.

b30. There are no safe haven measures for fax machines. However, there are plans to reduce the number of fax machines and control them in a central hub.

Recommendation: Minimise the access to fax machines to prevent any accidental disclosures, and implement the proposed secure printing measures.

Management response: **Agreed. The implementation of new multi-function devices will reduce the need for fax machines. These devices (MFD's) will not print until recipient inputs a user code. The Council is looking to reduce the number of fax machines in operation and move to more secure technologies over time.**

Implementation date: **June 2014**

Responsibility: **Iain Johnston \ Jacqui Dougall**

b31. There are no secure printing measures in place, although there is a project to introduce Multi-Functioning Devices (MFD). This will require users to input a pin to access print jobs.

b32. Where a new starter needs access to MC systems it is the responsibility of the new manager to contact IT with the requirements. There is a standard form that is completed for this. IT will then set up the basic account and contact any systems administrators for any further access that is required for their role.

b33. The main system forces a complex password of at least eight characters to be used. Passwords have to be changed every 90 days.

b34. Access to systems is restricted to the requirements of the role. Some of the systems are able to further restrict access to particular cases. They also allow for cases to be locked down so that only specific staff access can access them.

b35. Systems are reviewed to assess whether logons are still required. Access is removed if there has been no access for a set amount of time.

b36. Where a staff member changes role the new manager is responsible for completing the form if there are any changes to system access requirements.

b37. There is an Information Security Policy in place.

b38. Staff are required to lock their screens when away from their desks, but the system will automatically lock after ten minutes of non-activity.

b39. USB ports on desktops are all locked down, and will only accept approved devices. Sanctuary is used to restrict USB access. This produces logs for review should there be an incident, but they are not reviewed pro-actively as the controls are deemed adequate to block unauthorised access.

Recommendation: Ensure that where even unsuccessful attempts to transfer data take place they are highlighted and investigated

Management response: **Reject. The Council has introduced software designed to explicitly prevent data transfer to unauthorized USB devices. The product is CESG CCTM approved and deemed fit for purpose. The resource required to identify and then investigate unsuccessful attempts outweighs the benefits. Limited security resource would be better used elsewhere as agreed during the audit.**

Implementation date: **N\A**

Responsibility: **Information Security Officer**

b40. The system forces the use of encryption to any USB devices.

b41. There are no CD-DVD burners in machines unless there is an identified business need for them.

b42. The systems use hard drive PCs although they are considering moving to a VDi solution.

While it is possible to save material on the hard drive this is discouraged as it would not back up.

Recommendation: Consider disabling access to hard drives in desk top machines.

Management response: Accept. The Council will consider disabling access to hard drives as part of the PC desktop replacement program, although it's highly unlikely that it could ever be universally applied.

Implementation date: March 2014

Responsibility: Information Security Officer

b43. There is wireless access in the office which is configured to CESG standards and restricted to business use.

b44. Remote working is available to some staff and the requirements are formalised in the Remote Working Policy. For an individual to use remote working they have to get sign off from the director of Corporate Resources.

b45. MC uses CITRIX which provides an encrypted dual authentication method for staff to access systems and applications. Printing and copying facilities are disabled when users are logged on remotely.

b46. Remote working is reviewed every 12 months to ensure it is still required.

b47. Smartphones (Blackberrys and i-Phones) can be issued to staff where they are required for their role. They are encrypted and have kill codes in case they are lost or stolen.

b48. They are also locked down to prevent access to app stores.

b49. There were instances where council workers may have to take manual records out of the office. In these situations they were aware of the requirement to minimise the information taken and keep it secure.

b50. There are logs of web activity that are reviewed every week for unauthorised attempts to access forbidden sites.

b51. Anti Virus (AV) software is in place and updated regularly. Logs of anything the AV software catches are kept and reviewed.

b52. There are firewalls in place that are CESG approved and kept up to date.

b53. There is penetration testing included in an annual IT check. MC use an external company for this and a different company is selected each year. Firewalls are tested as part of the annual IT check.

b54. SCCM is used for patch management. They roll out new OS patches on a monthly basis. The log of patches highlights ones that are pending as well as those that are already implemented.

b55. Framework-i (Fi) has audit trails which record access to cases as well as any changes made. Team leaders are supplied with a sample of records that their team has accessed and asked to reconcile that the access was warranted. This is good practice.

b56. There are audit logs in place that provide trails to ensure any access was authorised. However, there is no standard monitoring and reporting that is used to provide the SIRO/ IMG with an overview.

Recommendation: Develop KPis for systems to provide the SIRO/ IMG with high level oversight of systems.

Management response: Agreed. Link to a22 for full response.

Implementation date: July 2013

Responsibility: IMG

b57. Cloud services are used for the front end of the email service as a security measure for incoming electronic communications.

7.3 Scope: Requests for personal data. The processes in place to respond to any requests for personal data. This will include requests by individuals for copies of their data (subject access requests) as well those made by third parties and sharing agreements.

Risk: Without a robust process for responding to formal requests for personal data there is a risk that personal data will not be provided in compliance with the DPA, resulting in regulatory action against the organisation and/or damage and distress to individuals.

c1. There is a management structure in place to ensure oversight of the handling of subject access requests (SARS). MC has received a low number of SARS since the process was implemented. This has an impact on the ability of MC to assure itself that it currently has effective oversight of data protection compliance when handling requests for personal data.

c2. Overall responsibility for ensuring the rights of data subjects are respected lies with the Head of Customer Services (who is also MC's Senior Information Risk Owner - SIRO).

c3. The IMG advises the SIRO on general data protection compliance including compliance with SARS requirements. IMG members are drawn from various areas within MC including legal, IT and service areas.

c4. Processing of SARS is not centralised. SARS are processed locally in the relevant service area and responsibility to do this is delegated from the Head of Customer Services to the Heads of Service.

Recommendation: Consider refining the existing SAR process so that there is more central oversight – for example centralised quality assurance. This will also enable a knowledge bank of best practice to be built up for reference by the service areas that may only infrequently come across SARS

Management response: Agreed. The SAR process is currently under review and recommendations will be integrated into the new procedure. Nominated officers for each division have been identified to monitor SAR's.

Implementation date: Jan 2014

Responsibility: IMG

c5. It was reported that key divisional contacts (reporting to the Heads of Service in each area) take on most of the processing of SARS in each service areas. These responsibilities do not appear to be formalised within role descriptions although in interview relevant staff demonstrated good awareness of their obligations.

Recommendation: Formally document role descriptions to clearly set out staff responsibility for processing SARS

Management response: Agreed. Role descriptors will be created for staff responsible for processing SAR's

Implementation date: Jan 2014

Responsibility: IMG

c6. The total numbers of SARS recorded as received across MC are currently low. In the service areas within scope (Criminal Justice, Revenues and Benefits and Travel Team) staff interviewed could not recollect receiving a SAR.

c7. There is corporate recognition of data subjects' rights to make a SAR. The MC website contains details of how to make a SAR and a copy of the relevant form. Auditors also noted that hard copy SAR forms were kept on some of MC's reception desks for provision to the public.

c8. The Travel Team incorporate advice to customers of the right to make a SAR in their renewal forms. This is good practice and MC may wish to consider using similar wording across other service areas.

c9. SAR volumes were observed to be very low across MC as a whole and in particular within the scope areas. In interviews it was explained that this may be because many requests for information were responded to as part of the normal course of business in line with MC's culture of transparency. Where requests are being dealt with as "business as usual" there is a risk that the requirements of compliance are not met.

Recommendation: Implement awareness raising training for staff on how to recognise if a SAR is being made, consider building on MC's existing freedom of information training modules (how to recognise a freedom of information request) to achieve this

Management response: An E-learning module will be created and training sessions conducted to increase awareness.

Implementation date: Jan 2014

Responsibility: IMG

c10. Interviews established that MC recognised it was important to ensure that all SARS received (whether on a form or within general correspondence) were recognised and logged to ensure accurate and timely logging and processing.

c11. Interviews with call centre staff established that although very few enquiries or requests about how to access personal data were received over the telephone for the areas within scope, they were aware of the on line form and IMG contacts within MC to speak to if they had a query or they needed to pass a SAR request on.

c12. MC has subject access policies and procedures reflecting its recently revised SAR process which were observed to be available to all staff via MC's Intranet. This was in line with ICO and DPA good practice except that that the SAR observed did not refer to guidance on how to apply exemptions.

Recommendation: See rec c26

c13. Interviews established that divisional contacts in each service area take on the SARS work, Heads of Service would only sign off the SARS. No SARS had been received by any of the scope areas as at date of audit and so auditors were unable to verify any process for sign off by Heads of Service.

c14. Where subject access requests may require cross-divisional searches for information, MC's IS04 Procedure for Handling Subject Access requests states at this point it may be useful to involve an IMG member. However, the Privacy Policy says that these are the responsibility of the Head of Customer Services.

Recommendation: Consider clarifying the process regarding dealing with SARS that involve cross divisional searches to ensure they are logged and processed correctly, in a timely manner, and that MC staff know who to pass them to,(perhaps a central resource such as the Data Custodian).

Management response: SAR process currently under review. Role and responsibilities will be clearly defined. A template has been developed outlining search areas and timescales to respond.

Implementation date: Jan 2014

Responsibility: IMG

c15. Interviews established that, while staff may have attended general training sessions (for example corporate induction), none of the key staff responsible for SARS or data sharing had received specialist role based training. Some training slides / materials are available on the Intranet which date back to 2008. These are kept for reference and are not used.

Recommendation: Ensure that key staff responsible for dealings with SARS, disclosures, redactions, exemptions and data sharing receive appropriate training and ongoing periodic refresher training which is logged centrally and monitored

Management response: Key staff will be trained in dealing with the more specialised aspects of DPA especially SAR's and data sharing.

Implementation date: March 2014

Responsibility: IMG

c16. Staff interviewed considered that they had ready access to either the legal department or members of the IMG should they have any queries.

c17. MC has recently implemented a tracking database which records the receipt and processing of SARS. SARS received by email or post are logged on to this database by the PA to the Director of Corporate Services.

c18. The tracking database was observed on site and contains a number of useful features such as the ability to "stop the clock" on the SAR 40 day response period until appropriate identification evidence was received by MC. There is also the facility to add notes regarding exemptions and redactions. SAR correspondence is held locally and not scanned onto the database.

c19. No SARS had been received or logged within the service areas audited. However, auditors observed that SARs from other areas had sometimes been recorded on the system on receipt and at other times when all identification evidence had been received by the local SAR administrator.

Recommendation: See C26

c20. There is currently no formal annual reporting of SARs statistics by the various service areas through the IMG function as required by MC's IS04 series of policies. It was explained in interview that this was because the SAR process has only recently been set up and the target date for the first report is June 2013.

c21. The MC SIRO and chair of the IMG have access to real time figures via the intranet based SARS tracking database.

c22. As there has not been any SARS received in the scope areas, in interviews it was explained that therefore currently there is no record maintained of redacted information, nor is there any quality assurance testing.

c23. MC's SAR procedures doc (IS04) provides advice regarding how to redact third party data manually. However, staff interviewed had not had experience of applying this policy and redacting SARs as so few were received. As SAR responses are processed locally there may be a risk that inconsistencies of approach regarding redaction may occur over time.

Recommendation: See C26

c24. Although the SAR tracking database does not have the facility to hold scanned copies of correspondence, auditors noted that there is scope to include brief notes about whether redactions have been made on the system, however in the sample reviewed from service areas outside scope this facility had not been used.

c25. As there has not been any SARS received in the scope areas, there are currently no records maintained of exemptions applied, or any legal basis for those exemptions.

c26. MC's IS04 Procedure for Handling Subject Access requests does not contain any detail advising administrators how to apply any exemptions. Auditors established in interview that the legal department will provide advice on the applicability of exemptions or the need to redact if requested. However, asking for legal advice was not mandatory.

Recommendation: Update procedure to include exemptions to DPA 98, how to apply them and suitable review process to ensure they have been correctly applied.

Management response: The SAR's procedure is currently being reviewed. revision's will include guidance on the application of exemptions including case examples such as Durant and Ezias etc.

Implementation date: Mar 2014

Responsibility: IMG

c27. Procedures for responding to third party requests for personal data (for example from the police) vary across the areas in scope.

For example :

- within Revenues and Benefits details of requests received and disclosures made are kept indefinitely in manual form (copy forms on file) but no record is kept of whether any requests are queried or challenged by MC.

- within the Travel Team disclosure requests are received over the telephone, responses are also made over the telephone and no record is kept.

- Criminal Justice has their own criminal justice investigation release form (with no version control) and a log is kept.

Recommendation: Introduce a consistent process for considering and responding to requests for personal data; both third parties and SARs. Include a requirement to record responses and partial responses given by MC to provide an audit trail. Include details in the records that demonstrate decisions disclosing or withholding information.

Management response: Sharing agreement documentation suite to be developed along with SAR process review, placing a greater emphasis on recording of actions etc.

Implementation date: March 2014

Responsibility: IMG

c28. Interviews established that across all areas there was no sampling or quality assurance of disclosures made. Interviews established that in some areas such as Revenues and Benefits advice would be obtained from the legal department regarding disclosures.

Recommendation: Introduce a method of quality assuring responses, such as dip sampling of a selection of responses by line managers to ensure that exemptions are being considered and applied correctly

Management response: Midlothian will sample 10% of SAR's and third party shares to ensure quality & consistency of response.

Implementation date: March 2014

Responsibility: IMG

c29. Some data sharing agreements were noted to be in place for each service area audited. Two were seen by auditors and were noted to be on MC's standard IS01 /IS02 forms. These cover issues recommended by the ICO such as appropriate security measures to be considered, whether the disclosee has signed a non-disclosure agreement, whether the sharing involves sensitive personal data, frequency and technical aspects of transfer, and retention and deletion considerations (see finding 40). However, currently MC is still in the process of identifying and logging all its existing data sharing agreements

c30. It was explained in interview that some data sharing (such as National Fraud Initiative and DWP sharing) were undertaken under national protocols rather than Council specific agreements.

c31. MC has recently produced new detailed guidance for preparing and implementing data sharing arrangements for new contracts. The guidance is available on the Intranet and was prepared by the IMG. In interview it was explained that this was based on the Welsh Accord on Sharing of Personal Information (WASPI) framework. The IMG Action Plan also has completion of these for existing service providers for example in Communities and Wellbeing as an action.

c32. It was reported in interview that where appropriate data subjects would be made aware of information sharing, for example via the client information sharing forms used in Criminal Justice; however in the majority of cases within the scope areas a relevant exemption to the obligation to provide fair processing information may be engaged (for example in Revenues and Benefits in the case where data sharing is to prevent or aid detection of crime or fraud). Some sample fair processing notices used within the scope areas were observed by auditors.

c33. MC's Data Sharing Best Practice contains a framework for Council employees to ensure that any sharing of information both internally and externally is compliant with current government legislation and Council policy. It has been revised to reflect the ICO data sharing code of practice and also refers to compliance with the Identity Management and Privacy principles produced by the Scottish Government.

c34. MC also has an Information Sharing Agreement procedure requiring consideration of appropriate security measures, whether the disclosee has signed a non-disclosure agreement, whether the sharing involves sensitive personal data, frequency and technical aspects of transfer, and retention and deletion considerations and has to be signed by a Director or Head of Service.

c35. The IMG Action Plan provides that all new services and contracts will use these new agreements. During interview it was established that each of the scope areas had historically differing procedures and forms in place for sharing personal data. These historic arrangements are being reviewed to bring them into line with new practice but this is currently behind target.

Recommendation: Ensure that the arrangements brought into are promoted and used across MC and monitor this via the IMG Action Plan

Management response: All recommendations highlighted by the ICO will be included in the IMG action plan. This will be monitored in Covalent with a nominated officer assigned to each action.

Implementation date: June 2013

Responsibility: IMG

c36. No one person or Board currently has central oversight of all current data sharing agreements across MC although it was established in interview that (as with other aspects of information governance) members of the IMG team would be asked for advice where deemed necessary

c37. During interview it was explained that MC is in the process of logging all information sharing arrangements across all scope areas with a view to collating them all on the Information Asset Register (IAR) that is currently being populated. Screen shots of the IAR were observed on site by auditors. This was an on going process as at the time of audit. It is intended that this will assist with mapping information flows across MC.

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 Paul Hamnett, ICO Good Practice.

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:

- Hillary Kelly
- Ian Wragg
- Neil McEvoy
- Phil Timoney