ABERDEEN
CITY COUNCIL

Internal Audit Report

Corporate Governance

Data Protection

Issued to:

Richard Ellis, Interim Director of Corporate Governance
Fraser Bell, Head of Legal and Democratic Services
Simon Haston, Head of IT & Transformation
Steven Whyte, Head of Finance
Craig Innes, Head of Commercial & Procurement
Jessica Anderson, Interim Legal Manager – Legal Services
Anne MacDonald, Audit Scotland

Date of Issue: September 2016 **Report No. AC1707**

EXECUTIVE SUMMARY

The Data Protection Act 1998 regulates the processing of personal data from which a living individual could be identified. Processing of data includes obtaining, holding, use and disclosure of such information. The Act applies to any computerised or manual records containing personal information about living and identifiable people, and requires that appropriate technical and organisational measures are taken to ensure compliance with the Act.

The objective of this audit was to review arrangements in place across the Council to consider whether Data Protection legislation is being complied with. This included a review of Data Protection governance; policies and procedures; staff training; information management; the use ICT equipment; contracts and contractor performance; data sharing; confidential waste; subject access requests and risk management.

In general, arrangements are in place to demonstrate compliance with the Data Protection Act 1998. Areas where improvements could be made include key performance indicators for monitoring staff training; guidance for information asset owners; tracking of ICT equipment throughout its life; use of Data Protection terms and conditions in third party contracts; and use of Information Sharing Protocols. Recommendations made in respect of these issues have been agreed.

1. INTRODUCTION

1.1 The Data Protection Act 1998 regulates the processing of personal data from which a living individual could be identified. Processing of data includes obtaining, holding, use and disclosure of such information. The Act applies to any computerised or manual records containing personal information about living and identifiable people, and requires that appropriate technical and organisational measures are taken to ensure compliance with the Act.

1.2 The objective of this audit was to review arrangements in place across the Council to consider whether Data Protection legislation is being complied with.

1.3 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Jessica Anderson, Team Leader - Governance - Legal Services and Simon Haston, Head of IT and Transformation.

2. FINDINGS AND RECOMMENDATIONS

2.1 Data Protection Act 1998 and Registration

2.1.1 The Data Protection Act (DPA) 1998 is the legislation that applies to 'Data Controllers'; that is individuals or organisations who determine the purposes for, and manner in, which personal data is processed. The DPA 1998 includes 8 Data Protection Principles of good practice to be followed when processing personal data as well as additional conditions to follow when processing sensitive personal information.

2.1.2 The Act also covers: the rights of individuals, defined as 'data subjects', whose personal data is being held; exemptions to the DPA 1998 such as safeguarding national security; registration requirements and obligations to notify the Information Commissioner; as well as offences and penalties.

2.1.3 The Act requires that every Data Controller who is processing personal information registers with the Information Commissioner's Office (ICO) unless they are exempt. Failure to register is a Criminal Offence. Registration requires the Data Controller to provide details of the information processed and the purpose for which it is held. This is then published on the ICO website which is available to the public for inspection. Registration must be renewed annually and requires the Data Controller to review the details of the existing registration and, where appropriate, amend and record any new processes and collection of information.

2.1.4 The Council is classified, and is registered with the ICO, as a Data Controller. Registration is updated on an annual basis on behalf of the Council's Data Protection Officer (Head of Legal & Democratic Services) by the Governance Team within Legal Services. The Council's current registration is shown on the ICO website.

2.1.5 The ICO notifies the Council when the annual registration fee is due to be paid. The Governance Team checks if there have been any changes to the categories of personal information processed or the purposes of processing. The SIRO will be notified of any changes through the Information Governance Group (see paragraph 2.3.2).

2.2 ICO Audit

2.2.1 The Information Commissioner is responsible for enforcing and promoting compliance with the DPA 1998. The Council invited the ICO to conduct an audit of the Council's compliance with the Act, known as a Good Practice Assessment, which was completed in June 2013. This found that there was a reasonable level of assurance that processes and procedures were in place and were delivering Data Protection compliance.

2.2.2 The audit focussed on three main areas: Data Protection governance, training and awareness, and the security of personal data, and highlighted both good practice and areas for improvement.

2.3 Data Protection Governance

2.3.1 Data protection governance is 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.

2.3.2 The Council has in place a clear framework of roles to meet its obligations under the Data Protection Act (DPA) 1998:

- The Head of Legal & Democratic Services is the nominated Data Protection Officer

(DPO) and also the nominated point of contact for the ICO. The Head of Legal & Democratic Services has overall responsibility for the Council's Data Protection Policy and Procedures. The role of the DPO is distinct from that of the SIRO and focuses on overall legal compliance with the Act.

- Previously, the Data Protection Technical Officer (DPTO) dealt with matters pertinent to ICT and Data Protection. The scope of the role of the DPTO has now been assumed within the wider and holistic role of the Senior Information Risk Officer (SIRO). The role of SIRO focuses on overall ownership of information risk management namely; information governance, risk management, risk assurance and compliance with information management and security. The SIRO's responsibilities are to lead a culture of good information management.

- There is an Information Governance Board made up of the SIRO, Information Manager and team, Security Architect, Risk Manager, and representatives from Communities, Housing and Infrastructure, Education and Children's Services, Integrated Health and Social Care, the Corporate Investigation Team and members of the Governance Team of Legal Services.

- Each Head of Service is responsible for adherence to Policy and Procedures by their staff. Each Service has an Information Management Liaison Officer (IMLO) who are responsible for providing support to all staff within their Service with respect to any Data Protection queries and are the first-point-of contact should queries arise. IMLO meetings are held every 6 months and one of the agenda items is Data Protection.

- The Governance Team within Legal Services provide detailed advice, assistance and training on Data Protection matters to the IMLOs and Services across the Council.

2.3.3 Data Protection compliance has been reported on a quarterly basis to the Audit, Risk & Scrutiny Committee, as a result of the recommendations made by the 2013 ICO Audit. As part of a wider Governance Review in 2016, the Council is reviewing its arrangements for managing and reporting on Information Governance. As a result of this review the Council is now proposing that compliance with the DPA is also reported quarterly to the Corporate Management Team (CMT) as part of a wider overview of compliance on Information Governance, which encompasses, Data Breaches, Subject Access Requests, Freedom of Information Statistics, Data Incidents, Security Management and Records Management. The report proposing these new arrangements, and including a quarterly compliance update, was considered by the CMT in July 2016, and is scheduled to be considered by the Audit, Risk & Scrutiny Committee in September 2016.

2.3.4 The 2013 ICO audit recommended that a formal Data Protection strategy, including information management and information security, should be written and implemented as soon as is practicable. The ICO went on to advise that this should identify a steering group, attended by appropriately senior subject matter experts, in order to achieve satisfactory corporate oversight. It was agreed the Information Management Strategy and Action Plan would be updated by August 2013 to cover this. The Council set up a corporate information management advisory group (IMAG) to facilitate the implementation of the wider Information Management Strategy.

2.3.5 As a result of the Council's review of its arrangements for managing and reporting on information governance, an Information Governance Board was established in May 2016, which will replace the IMAG in respect of responsibility for driving the Council's required programme of work for Data Protection compliance. The Information Governance Group is currently undertaking a review of Data Protection compliance including systems and processes, training and awareness and breach reporting.

2.4 Written Policies & Procedures

2.4.1 The Council has a clear and concise Data Protection Policy, located on the Zone. This explains the need for such a policy, and sets out the Corporate Data Protection Framework of roles and responsibilities in order to meet the requirements of the DPA 1998. This includes the duties and responsibilities of all staff with regard to the DPA 1998 including the specific roles of Service Information Management Liaison Officers (IMLO); Service Data Protection Technical Officers (DPTO); the Head of Legal & Democratic Services; All Heads of Service and Elected Members. The policy also covers training; disciplinary matters; registration responsibilities with the ICO for the Council and Elected Members; how information should be managed during its lifecycle; and when things typically go wrong.

2.4.2 As reported in Internal Audit report AC1604, Corporate Policies and Procedures, the Council has several individual procedures supporting the Data Protection Policy. These are attached in the appendix to the Policy

2.4.3 It has been identified that there are links to older versions of the policy and procedures which exist within other policies on the Zone which may be confusing for staff as older superseded versions may conflict with the most recent versions.

Recommendation
A review should be undertaken of the documents on the Zone to ensure there are no conflicting policies / procedures and to ensure that only the current version of procedures is available to view.

Service Response / Action
Agreed. This will be picked up as part of the wider Information Governance Group review.

Implementation Date	Responsible Officer	Grading
March 2017	Public Performance Reporting and Digital Engagement Manager	Important within audited area

2.5 Training

2.5.1 The Council's Data Protection Policy requires all staff who process personal information to undertake specified Data Protection Training at the commencement of their employment and also to complete regular refresher training thereafter. The introduction of refresher Data Protection Training was also one of the recommendations within the ICO's 2013 Audit Report, which the Council accepted.

2.5.2 The Council has three Data Protection related training courses – 'Data Protection – Essentials', which focusses on Data Protection, the recently introduced E Induction which covers core Council policies for new employees, and 'For Your Eyes Only', focussed on Information Security. There is also face to face and paper based training which is available to staff who do not use a computer, or staff who are not required to complete the full training due to the requirements of their job.

2.5.3 Management reports were requested to show completed and outstanding Data Protection training however such reports did not provide clarity or assurances on compliance in relation to all formats of Data Protection training and it was not clear how non-compliance was managed.

2.5.4 The ICO recommended in its 2013 Audit Report that reporting improvements should be

implemented in relation to the monitoring of training completion, in order to simplify the identification of staff who have not undertaken mandatory training within an acceptable period. The ICO also recommended that formal Key Performance Indicators (KPIs) be introduced, overseen by CMT, to formally measure mandatory Data Protection training completion.

2.5.5 Organisational Development within Human Resources have implemented changes to the Induction Checklist which requires managers to identify what level of Data Protection training is required for the post. Further, employees will be asked to confirm that they have received and understood messages in respect of core policies through the Performance, Review and Development programme. In July 2016, the Interim Director of Corporate Governance sent round a reminder to staff to update their Data Protection knowledge. This stated that Data Protection training is a mandatory requirement for all staff and requested that managers should ensure all staff have completed the appropriate level of training. Where the Data Protection Essentials course had been completed in the last 12 months there was no requirement for further action. Where the Data Protection Essentials course has never been completed this course or the E-Induction needed to be completed by October 2016. E-induction is a recently developed mandatory course for new employees covering core policies including Data Protection. Reports on completion of the Data Protection module training have been sent to managers in July and August 2016 to show the compliance of Data Protection training and work is ongoing in respect of staff who do not use a computer, which will require them to confirm they are aware of and understand their responsibilities in respect of Data Protection.

2.5.6 The ICO recommended in the 2013 Audit Report that a training course specific to Subject Access Requests should be implemented. The Governance Team in Legal Services confirmed face to face training is provided to Services on bespoke issues (monthly training on Adult Protection and Information Sharing, Information Sharing training to City Wardens, and annual training to the Educational Psychology Service). In addition, the Service confirmed that in March 2015, due to a change in personnel, the Complaints, Rights and Enquiries Team in Social Work had specialised training on Subject Access requests and Third Party Request procedures and a specialised presentation was developed for that training. The Service has also advised that the training reflects the current guidance from the ICO and is compliant with the Council's current procedure. Refresher Training has been identified as a priority by the Information Governance Group though it will focus on more practical advice / tips for staff about good information management.

Recommendation

The SIRO should work with all relevant Services to develop and deliver all appropriate Council staff with refresher training which includes the areas of Data Protection related information security and information management standards, on a three yearly basis.

The SIRO should consider what appropriate measures should be implemented to measure all forms of Data Protection training. As per the recommendation made by the ICO in its 2013 Report, formal KPIs, overseen by CMT, should be introduced to measure mandatory Data Protection training completion. Additionally, this should also include how instances of non-compliance shall be dealt with.

Service Response / Action

Agreed. Issues around the uptake and recording and reporting on the uptake of mandatory training are being investigated and reviewed by the Information Governance Group as a priority.

Implementation Date	Responsible Officer	Grading
March 2017	Information Manager	Significant within audited area

2.6 Records Management

2.6.1 The Council's Information Management Team maintains an Information Asset Register, which records all information assets (of which the Information Management Team have been advised). This should allow the Council to ensure all information and personal data is managed (stored, used, distributed, disposed of) correctly as per the DPA 1998.

2.6.2 The Information Asset Register is still fairly new in the Council and the Information Management Team understands that further work is required to develop the register to ensure all Services advise them of new / changed information to allow updating of the register. This will allow the register to be used as a management tool to identify high risk areas for further assessment and attention.

2.6.3 The Information Asset Register links to the Council's Records Retention & Disposal Schedule via the Council's Business Classification Scheme and this allows the two to be linked and appropriate retention and disposal triggers, dates, rationales to be understood for each asset. The Records Retention & Disposal Schedule also provides guidance on how different types of information should be disposed of. The Council also has in place Corporate Information Management Procedures for staff which gives guidance on managing information appropriately throughout its lifecycle.

2.6.4 It is the responsibility of each individual Information Asset Owner to manage their piece of information including, for example, ensuring the information is used only for the purpose(s) specified. Services also have file plans in place which set out what information each team has, where it is, and how long it should be kept for. These are at different stages of maturity, and will be further embedded and developed with Information Asset Owners as part of the IGG Improvement Programme.

2.6.5 The Information Asset Register Policy sets out the roles in relation to managing Information Assets. These roles will be further developed and embedded as part of the Information Governance Group's improvement programme.

Recommendation
The Service should embed and develop roles and responsibilities of Information Asset Owners with supporting guidance as appropriate.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
September 2017	Information Manager	Significant within audited area

2.7 Protective Marking Scheme

2.7.1 In the 2013 Audit Report, the ICO recommended that the Council adopt a protective marking scheme so as to provide clear benchmark guidance for appropriate security standards to apply to any data being processed. The Council advised that they would undertake an options appraisal to assess whether a Protective Marking Scheme would be adopted.

2.7.2 As per the Council's June 2014 update document to the ICO (detailing progress made against each of the ICO recommendations), progress on implementing this recommendation had been delayed due to wider issues in respect of the government marking scheme. An options appraisal was to be carried out including considering the new Government Classification Scheme with two markings that could be used –

'OFFICIAL' and 'OFFICIAL SENSITIVE'.

2.7.3 The ICO further recommended that protective markings should be applied to data and follow to 'end of life' including occasions of further processing.

2.7.4 From discussion, it was advised that the Government Classification Scheme has been piloted within Social Work. It has not been decided whether the Scheme will be fully rolled out within the Council.

Recommendation
The Council should conclude work on the options appraisal following the Social Work pilot and roll the Scheme out to all other Services, if appropriate.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
March 2017	Information Security Architect	Important within audited area

2.8 ICT Equipment

2.8.1 Breaches of Data Protection can involve the loss of computers, laptops and USB memory sticks. The security arrangements in place were reviewed for adequacy.

2.8.2 ICT assets are recorded on the Council's Corporate Asset Register, where asset numbers are allocated and the make, model, serial number, user, service, location, PO number, PO date, cost and input date are recorded. Where the end user of the equipment is not known, the name of the person placing the order may be recorded as the user. In addition, the location may not be entered if this is not known.

2.8.3 The Corporate Asset Register is not updated during the life of the equipment. From testing a sample of 30 former employees, laptops are still assigned to 4 individuals who no longer work for the Council.

2.8.4 The Council went through an exercise in 2012 to upgrade and replace all Council owned laptops where necessary to allow for disk encryption to take place. This exercise was completed and all laptops are encrypted with the exception of one old Art Gallery laptop which is being used for presentations only.

Recommendation
Consideration should be given to using the Corporate Asset Register to track IT equipment throughout its life, recording current status, owner and location.

Where the name of the end user or location is not known, notes explaining the situation should be recorded in the Register.

Service Response / Action
Agreed. A Service Management Tool is scheduled to go live in October 2016. This will contain an Asset Management module for tracking IT equipment.

Implementation Date	Responsible Officer	Grading
March 2017	IT Customer Services Manager	Significant within audited area

2.9 Access Controls – Leavers or Movers

2.9.1 IT are notified retrospectively of personnel who have already left, through a monthly spreadsheet provided by HR. This creates a potential risk that staff who have left the Council can access Council systems during the month following their leaving date.

2.9.2 There is no formal procedure surrounding return of leavers' ICT equipment to IT. The online Leavers Form reminds leavers to return ICT equipment but there does not appear to be a requirement for Line Managers to return the equipment to IT. On discussion with IT & Transformation, the leavers' ICT equipment is handled by the exiting employee's Line Manager.

2.9.3 It is not clear whether individual Services consistently advise IT regarding any changes to an employee's role. There does not appear to be a documented requirement for Services to advise ICT of such role changes.

Recommendation
ICT should work with HR&OD to develop and introduce a clear procedure surrounding leavers including, for example, notification to IT of the scheduled leaving date (to allow for disabling of their account on the leaving date) and return of ICT equipment to IT. The procedure should also set out the requirements surrounding personnel role changes including promotions and secondments.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
January 2017	IT Technology Manager	Important within audited area

2.10 User Accounts

2.10.1 The Service undertakes regular checks for dormant network user accounts.

2.10.2 The Service has in place ICT Operations Standards, including guidance on the processes for setting up user accounts. The Service advised that there is a process of risk assessment in place before a generic user account is set up but this is not explicitly documented in the ICT Operations Standards.

Recommendation
Current ICT Operations Standards should be updated to document the processes in place surrounding the use of generic network user accounts.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
December 2016	IT Technology Manager	Important within audited area

2.11 ICT Acceptable Use

2.11.1 The ICT Acceptable Use Policy provides a high level overview of acceptable use of ICT equipment. The Policy defines unacceptable use and provides some guidance surrounding passwords, personal use of Council ICT equipment, systems and networks, system back-ups, access and monitoring; and breaches and incidents reporting.

Corporate Information Management Procedures are available to staff which cover use of encrypted ICT equipment, remote working, email guidance and general good practice guidance on managing information throughout its lifecycle.

Recommendation
Consideration should be given to updating the ICT Acceptable Use Policy to include links to other ICT procedures.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
December 2016	Information Manager	Important within audited area

2.12 Contracts & Contractor Performance

2.12.1 The Council has agreements in place with a number of third parties who have access to the data for which the Council is responsible, as Data Controller. It is important that adequate Data Protection and Confidentiality Terms & Conditions are in place (either within the main contract with the third party or as a separate agreement) to ensure protection of this data and compliance with the Data Protection Act 1998.

2.12.2 Employees have an implied duty of confidentiality under the terms of their contract of employment and Code of Conduct (see Clause 7.6 - Confidential Information) and are required to comply with the DPA 1998 without the need to sign a confidentiality agreement. Non-employees, include agency staff engaged outwith a framework agreement, volunteers, placement students and contractors, who process personal data on behalf of a Data Controller and are classed as Data Processors under the DPA 1998. Only Data Controllers are obliged to comply with Data Protection legislation and are responsible for any processing undertaken by their Data Processors. Non-employees who will potentially have access to personal or sensitive data must therefore sign a confidentiality agreement. Where staff are provided by a third party supplier which the Council has a contract or approved framework agreement with, the third party organisation providing the staff is deemed to be the Data Processor and is required to sign a confidentiality agreement rather than the individual staff members.

2.12.3 A sample of 12 suppliers with access to personal data was selected in order to establish valid contracts and confidentiality agreements are in place and that the Council is monitoring contract performance to ensure terms and conditions are being complied with. Information was unavailable for 5 of the 12 sampled suppliers. Of the 7 provided, 1 of the contracts relating to residential care services has not been signed. The remaining contracts provided are valid and include within them Data Protection and confidentiality terms and conditions.

2.12.4 CPS have developed a contracts register in collaboration with Services. However, contracts selected for testing were not stored centrally and instead were held by the respective Services. It has proven difficult for staff to locate contracts. This would suggest that contract management, including monitoring expiry dates, could be difficult.

2.12.5 One of the contracts requested was agreed 18 years ago and it was advised that there has since been only a single two and half year extension. It has not been possible to obtain a copy of the original contract to verify the agreed contract term but there is a risk that work has been carried out without a valid contract in place.

2.12.6 A plan of audits to be carried out on supplier performance was requested. Such audits

are beneficial for ensuring the terms of a contract are being complied with. The plan has not been provided and since no reports have been provided, it would appear that audits of contract compliance have not been carried out on any of the 12 sampled contractors.

Recommendation
Work should not be carried out with a third party without a valid, signed contract in place.

Services should be advised to seek the advice of the Legal Team within CPS, when engaging with a new supplier to ensure appropriate Data Protection clauses are included in the contract.

The Council should exercise their contractual rights to carry out contract compliance audits to provide assurance of Data Protection Act compliance.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
March 2017	Team Leader, Legal Team, Commercial and Procurement Services	Important within audited area

Recommendation
Contracts and supplier evaluations should be stored centrally, easily accessible and regularly reviewed in order to ensure effective contract management, including monitoring of expiry dates, exercising rights under the contract (such as the right to perform an audit) and ensuring fulfilment of contractual obligations.

Service Response / Action
Agreed

Implementation Date	Responsible Officer	Grading
April 2017	Head of Commercial & Procurement	Important within audited area

2.13 Data Sharing

2.13.1 Data Sharing refers to the disclosure of data from one (or more) organisation(s) to a third party organisation, or the sharing of data between different parts of an organisation. As well as one-off decisions to share data for any range of purposes, data sharing covers systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose. Data sharing primarily refers to the sharing of data between data controllers (rather than between a data controller and data processor – which requires a written contract with specific Data Protection terms and is covered in 2.12 above).

2.13.2 Testing of an example ACC Memorandum of Understanding and associated Information Sharing Protocol confirmed that the ISP is in accordance with the principles of the Data Protection Act 1998.

2.13.3 From discussion however, it was advised that ISPs may not always be sent to Legal prior to implementation.

2.13.4 As per the Corporate Data Protection Procedure – Routine Data Sharing Procedure, if any routine sharing of personal data is to take place with an external agency then the Head of

Legal and Democratic Services has to be informed as soon as possible and a legally binding Information Sharing Protocol must be entered into with the external parties. Advice must be sought from the Head of Legal and Democratic Services prior to an ISP being signed.

2.13.5 In its 2013 Report, the ICO recommended that a central log of data sharing instances be created and implemented, which should include occasions where Data Protection Act 1998 s29 and s35 exemptions are engaged. Section 29 allows disclosure of personal data for the purpose of preventing/detecting crime, for apprehending/prosecuting an offender and for assessing/collecting a tax or duty (where informing the data subject(s) may prejudice an investigation). Section 35 allows disclosure of personal data where there is a law or court order requiring the information or where it is necessary in connection with legal proceedings.

2.13.6 Despite the Council's update to the ICO in June 2014 (reporting on progress made against each of the recommendations) stating that a central log was now being maintained, it has not been possible to verify that a central log of data sharing instances has been implemented. Legal Services confirmed that they do not hold a central log since each Service maintains their own data sharing log. Services retain information about third party data sharing and these statistics are collated and provided as part of a quarterly report to the Audit, Risk and Scrutiny Committee.

Recommendation
Services should be reminded of the requirement that advice must be sought from Legal and Democratic Services prior to Information Sharing Protocols being signed.

As per the ICO recommendation in its 2013 Audit Report, consideration should be given to implementing a central data sharing log which includes all agreed Information Sharing Protocols.

Service Response / Action
Agreed. Work should be done to investigate the possibility of all Services using the same database so that statistics recorded by Services on Subject Access and Third Party Request compliance can be accessed centrally for reporting purposes.

Implementation Date	Responsible Officer	Grading
March 2017	Interim Legal Manager – Legal Services	Significant within audited area

2.14 Confidential Waste

2.14.1 There is a shared contract with Aberdeenshire Council engaging an external company to manage the Council's confidential waste. The company securely collects confidential waste and shreds it in their secure vehicles before obtaining a signature from Council staff on the Certificate of Destruction and transporting the shredded material to their depot, where it is baled and then recycled. The Contract adequately addresses Data Protection but it only states that the contractor must comply with Aberdeenshire Council's Data Protection Policies and does not mention Aberdeen City Council's policies.

2.14.2 No audits have been carried out of the contractor and minutes are not formally recorded at performance management / contract compliance meetings. Regular performance management / audits would be beneficial to ensure continued satisfactory performance as recommended in Section 2.12.

2.15 Subject Access Requests

2.15.1 The 'Right to Subject Access' is the right of individuals under the Data Protection Act 1998 to establish if data controllers are processing information relating to them and the purposes for which it is being processed. As per the legislation, any requests for such information must be responded to within 40 days.

2.15.2 8 Subject Access Requests were made to Communities, Housing and Infrastructure in the last 6 months. As per the Data Protection Act 1998, data controllers may charge a fee in return for responding to a Subject Access Request. A fee was not charged for 7 of these requests. Where fees were not charged, the reason for not charging has not been recorded.

2.15.3 There may be confusion surrounding the charging of fees for subject access requests. The 2015 procedure states that all Services have their own guidance surrounding the charging of fees. The 2012 procedure (also accessible on the Zone) states that consideration should always be given to not charging a fee, if appropriate. Section 2.4, above, already recommends that a review be undertaken of version control of procedures stored on the Zone.

2.15.4 In the last 12 months, 63 of the total 84 subject access requests received by the Council were responded to within the legislatively prescribed 40 days. The late responses were largely due to extensive staff time and resource involved in examining multiple voluminous records to remove third party data and make appropriate redactions.

2.15.5 The 2013 ICO audit recommended that a dedicated Subject Access Request training course, written at a suitably detailed level, be devised and rolled out to appropriate Council staff. The Council had identified the need for such training including the intricacies of exemptions applications and third party requests prior to the 2013 ICO audit. The ICO recommended the training should be implemented by January 2014. As noted at 2.5.8 above, a dedicated module on subject Access training was developed and was delivered in March 2015 to the Complaint, Rights and Enquiries Team within Social Work and the respective Council procedure, approved in September 2015, reflects up to date guidance from the ICO in relation to handling of subject access requests.

2.15.6 There does not appear to be a central log of Subject Access Requests. All subject access requests are logged by individual Services, being the relevant Service holding and processing the data. The Governance Team in Legal Services collates data from Services and analyses the types of data, number of requests compared with other quarters, trends and response times. In the 2013 Audit Report, the ICO also recommended that controls be implemented to ensure that all subject access requests are centrally recorded. The Council accepted this recommendation but following requests for a copy of the central log, it was advised that each Service maintains its own log and there is not a central one. Rather, core datasets from each Service on subject access compliance are collated, analysed and reported on by the Governance Team, within Legal Services.

Recommendation
Clear guidance should be introduced surrounding charging fees for Subject Access Requests.

As per the ICO recommendation, the Council should consider implementing a central log of Subject Access Requests.

Service Response / Action
Agreed. It is noted that the charging of the Subject Access Fee is not consistent across the Council and the Governance Board will be considering whether the fee should be

waived for all requests or, if a fee is to be charged, develop guidance for staff on when the fee is to be applied.		
Implementation Date	**Responsible Officer**	**Grading**
March 2017	Interim Legal Manager – Legal Services	Important within audited area

2.16 Risk Management

2.16.1 Data Protection has been included as a general risk within the Corporate Governance Risk Register and work has commenced on the mitigating actions – for example, the Information Governance Board has been established.

2.16.2 An Information Governance Risk Register is being finalised as one of the Information Governance Board's actions.

2.16.3 A report on 'Data Protection Reporting (April 2015 – March 2016)' went to the Audit, Risk and Scrutiny Committee on 27 June 2016. The Management of Risk section of the report states the importance of compliance with the legislation and of monitoring compliance but does not provide any detail surrounding the results of such compliance monitoring in practice.

AUDITORS: D Hughes
M Beattie
A Johnston
A Mitchell

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the Council.
Major at a Service Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.