Internal Audit Report
Chief Executive's Service
Data Protection
Assignment No 14-07
November 2014

Final Report

Chief Executive's Service
Finance Division
Perth & Kinross Council
2 High Street
Perth PH1 5PH

Background and Introduction

This audit was carried out as part of the audit plan for 2014/15, which was approved by the Audit Committee on 2 April 2014. Audit testing took place in August and September 2014. The purpose of the audit was to review the adequacy of the Council's arrangements for Data Protection.

The Data Protection Act 1998 regulates the processing of information relating to individuals, including the obtaining, holding, use and disclosure of such information. It requires that appropriate technical and organisational measures shall be taken by organisations holding personal data to ensure compliance with the Act.

The Council has two policies in place, namely the Data Protection Policy and the Policy on Records Management & Preservation of Archival Records. These policies incorporate the Council's assigned responsibilities under data protection legislation. The Data Protection Policy states that:

- The Head of Legal Services is responsible for developing, publishing, maintaining and administering the Data Protection Policy;

- Executive Directors are responsible for all aspects of compliance with the Act and associated legislation within their Services. They may, however, delegate their data protection responsibilities to individuals or service providers;

- The Head of Legal Services will designate a Data Protection Officer who will develop appropriate procedures, strategies, codes of conduct and guidance and will oversee a management framework with the purpose of controlling adherence to the Data Protection Act 1998 within the Council.

The Data Protection Policy forms an integral part of the Council's Information Security Management System (ISMS). The ISMS further stipulates that the Executive Director (The Environment Service) has been designated the Senior Information Risk Owner (SIRO) for the Council.

An Audit Scotland report of August 2013 regarding the Review of Data Management included an agreed action plan that a revised e-Learning module for Data Protection be implemented. This action plan will be monitored through Internal Audit's 'follow up' arrangements and therefore not referred to in this report.

Acknowledgements

Internal Audit acknowledges with thanks the co-operation of D Henderson, Information Compliance Manager and Service based staff during this audit.

Control Objectives and Opinions

This section describes the purpose of the audit and summarises the results. A 'control objective' is a management objective that requires the maintenance of adequate and effective internal controls to ensure that it is achieved. Each control objective has been given a rating describing, on the basis of the audit work done, the actual strength of the internal controls found to be in place. Areas of good or poor practice are described where appropriate.

Control Objective: To ensure the measures currently adopted by Perth & Kinross Council in processing information relating to individuals are adequate. The work will focus on the arrangements currently in place and how effectively these arrangements are implemented within services.	
The Council's data protection policy adequately sets out the Council's data protection measures. The policy states that the Council policy is to full comply with the Data Protection Act 1998 and all other related statutory, criminal and civil obligations. The policy applies to all employees and Elected Members and compliance with the policy and associated procedures are a condition of employment. The latest published version of the policy was approved by the Executive Officer Team in February 2014 and thereafter by an Executive Sub-Committee of the Strategic Policy Resources Committee. The Head of Legal Services is responsible for designating a Data Protection Officer to develop appropriate procedures and this has been allocated to the Information Compliance Manager. The data protection policy requires an annual return from Services on the use and processing of personal information however there was no evidence that this had occurred. The policy also states that the Council will ensure that it maintains its notification entry with the Information Commissioner on an annual basis and the audit confirmed this to be the case. Testing of a small selection of Service based staff demonstrated an awareness and understanding of the data protection arrangements and the processes to be followed if an individual asks for a copy of information that the Council holds about them. There is scope to improve the adequacy of arrangements relating to the classification and disposal of 'confidential' waste. In addition, there is scope to improve arrangements to ensure that Scottish Government's data protection guidance for planning authorities is fully implemented. There is also scope to update the policy to ensure that it aligns with current practice regarding the sharing of information with outside agencies and to improve clarity.	
Strength of Internal Controls:	Moderate

Management Action and Follow-Up

Responsibility for the maintenance of adequate and effective internal controls rests with management.

Where the audit has identified areas where a response by management is required, these are listed in Appendix 1, along with an indication of the importance of each 'action point'. Appendix 2 describes these action points in more detail, and records the action plan that has been developed by management in response to each point.

It is management's responsibility to ensure that the action plan presented in this report is achievable and appropriate to the circumstances. Where a decision is taken not to act in response to this report, it is the responsibility of management to assess and accept the risks arising from non-implementation.

Achievement of the action plan is monitored through Internal Audit's 'follow up' arrangements.

Management should ensure that the relevant risk profiles are reviewed and updated where necessary to take account of the contents of Internal Audit reports. The completeness of risk profiles will be examined as part of Internal Audit's normal planned work.

Feedback

Internal Audit welcomes feedback from management, in connection with this audit or with the Internal Audit service in general.

Distribution

This report has been distributed to:

B Malone, Chief Executive

J Valentine, Executive Director, the Environment Service and Senior Information Risk Owner

J Fyffe, Depute Chief Executive and Executive Director, Education and Children's Service

J Walker, Executive Director, Housing and Community Care

B Renton, Depute Director, the Environment Service

I Innes, Head of Legal Services

K McNamara, Head of Environmental and Consumer Services

A Taylor, Head of Finance and Support Services, Housing and Community Care

D Littlejohn, Head of Planning and Regeneration

N Brian, Development Quality Manager, the Environment Service

D Henderson, Information Compliance Manager/Data Protection Officer

J Symon, Head of Finance

G Taylor, Head of Democratic Services

P Dickson, Complaints & Governance Officer

External Audit

Authorisation

The auditor for this assignment was D McCreadie. The supervising auditor was M Morrison.

This report is authorised for issue:

_____

Jacqueline Clark
Chief Internal Auditor
Date: 5 November 2014

Appendix 1: Summary of Action Points

No.	Action Point	Risk/Importance
1	Data Protection Policy and Procedures	Low
2	Subject Access Requests	Medium
3	Disposal of Confidential Information	High
4	Records Management Policy	Medium
5	Scottish Government Guidance for Planning Authorities	High
6	Data Protection Registration Entry	Low
7	Data Sharing	Low

Appendix 2: Action Plan

Action Point 1 - Data Protection Policy and Procedures

The Council's intranet site includes the Council's data protection policy and procedures. There is scope to improve the following aspects of this:

The policy refers to the role of the data protection officer. Whilst this job holder is in reality the Information Compliance Manager, the designation of data protection officer is not stated on the Legal Services intranet page, which makes it less easy for staff to identify that person. Audit testing of 6 randomly selected staff revealed that 3 staff could not identify the name of the data protection officer.

The data protection intranet page would benefit from a narrative detailing the linkage to the Council's information compliance team.

The policy and procedures refer to personal data, but fail to define the term personal data.

In addition, Education & Children's Services have their own data protection procedures. However, hyperlinks from their procedures open an out of date data protection policy.

Management Action Plan

a) The Information Compliance Manager will update the various Legal Services' intranet pages to ensure that they provide clear information regarding data protection responsibilities this will include for example, a statement that the Information Compliance Manager is the Council's designated data protection officer.

b) The data protection policy will be amended at the next opportunity to make it clear that the term "personal data" has the meaning defined in the Data Protection Act.

c) The Information Compliance Manager will liaise with Education and Children's Services to ensure the hyperlinks open the current policy.

Importance:	Low
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	a) November 2014 b) March 2015 c) November 2014

Required Evidence of Completion:	a) Updated Eric Data Protection page b) Updated Data Protection policy c) Updated Education & Children's Services procedures

Auditor's Comments

Satisfactory

Action Point 2 - Subject Access Requests

The data protection policy and the freedom of information (FOI) team's subject access request (SAR) procedures refer to the statutory processing period for such requests as 40 days but not 40 calendar days as per the Information Commissioner's Office code of practice. The Service advised that the FOI team were aware that the processing time related to calendar days.

There is no SARs guidance for staff based in the Services. The data protection officer advised this is because SARs should be directed to the FOI Team. However, this is not detailed on the relevant Eric page.

Also, an EOT report of 4 February 2014 agreed to the phased centralisation of subject access requests processing to the FOI team by the end of March 2014. This follows a review which was as a result of a commitment given to the Information Commissioner and arose from highlighted failures. The data protection officer advised that at the date of audit testing (September 2014) the centralising had not been completed.

Management information relating to SARs processing time is produced, but not currently distributed to any Group for review and analysis. The Service advised that the circulation and review of such will commence once the centralising of processing is delivered. As at the 22 September 2014, 94% (29) of the 31 recorded SARS requests were listed as responded to within the 40 calendar day period.

Management Action Plan

a) The published procedures for SARs will be amended to reflect the current situation regarding the processing of such requests. The FOI Team's procedures will be amended to reflect that the period is 40 calendar days rather than 40 working days.

b) The Information Compliance Manager will amend the data protection policy at the next opportunity.

c) The centralisation of the processing of subject access requests is dependent on the availability of adequate resources in the FOI team. An additional FOI Officer is currently being sought. This will be completed by March 2015 or an update report will be provided to EOT.

d) Management information about the processing of SARs will be reported when the centralisation of processing has been completed.(subject to the above)

Importance:	Medium
Responsible Officer:	D Henderson, Information Compliance Manager

Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	a) November 2014 b) March 2015 c) March 2015 d) March 2015
Required Evidence of Completion:	a) Updated SARs procedures for Services and updated FOI Team's procedures. b) Updated Data Protection policy. c) Evidence processing SAR's centralisation complete or EOT report. d) Evidence SAR's management information reported (subject to the above)

Auditor's Comments

Satisfactory

Action Point 3 - Disposal of Confidential Information

The Council's Information Security Standards contains guidance on the disposal of confidential information and arrangements are in place throughout the Council for this. However there is scope to improve these arrangements in that:

- The "confidential paper" section of the above standards state that employees must ensure the storage and transportation of such before destruction is "appropriate" to ensure that the "confidentiality" of the information is maintained. The standards however, do not define the term "confidential" which may result in the staff misinterpreting the requirements. There is also benefit in defining the term "appropriate" as audit testing revealed confidential waste is being stored within Services in plastic bin bags marked confidential, pending collection.

- The Council's Waste Services are responsible for the initial uplift and disposal of bulk confidential waste, which is ultimately shredded by an external contractor. There is no record of the number of bags containing confidential waste leaving Pullar House or 2 High Street on route to the depot at Friarton. Nor is there is any record of the number of bags transferred by Waste Services to the external contractor. Payment for the disposal of confidential waste is based on evidence provided by the contractor of the weight of paper being recorded at the contractor's weighbridge. As such, there is no assurance that all bags identified as containing the Council's confidential waste are destroyed.

The code of practice for secure document shredding, provided by the external contractor includes the provision of confidential waste bags and numbered tag seals; however this routine is not adopted by the Council.

In addition, interim guidance entitled the disposal of confidential information dated August 2008 is still available on Eric even though it has been superseded.

Management Action Plan

a) The disposal of confidential information guidance has been removed from Eric. This will be replaced with new guidance related to the Council's information security classification standards which will ensure that documents for disposal are properly stored and destroyed.

b) The Information Compliance Manager will liaise with Waste Services Manager to agree a confidential waste process which provides assurance that confidential waste has been correctly stored and destroyed.

Importance:	High
Responsible Officer:	D Henderson, Information Compliance Manager

Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	(a) and (b) December 2014
Required Evidence of Completion:	a) Updated confidential waste routine b) Guidance regarding storage and disposal of data

Auditor's Comments

Satisfactory

Action Point 4 - Records Management Policy

The records management policy states that it aims to ensure the Council complies with all legal and regulatory requirements including the Data Protection Act. The Council's information security standards further state that if confidential paper forms part of a Council record, then the appropriate procedures must be followed prior to disposing of the paper. However, the records management policy makes no reference to these standards.

There is benefit in clarifying when records can be destroyed as the above policy states that retention schedules will be drawn up by each Service and agreed after consultation with the Records Manager and Legal Services. Eric guidance accessed from the same page states that on 1 July 2011, the Council's policy and governance group approved the adoption of the Scottish Council on Archives Records Retention Schedule. A Frequently Asked Questions page on the Eric Data Protection page refers to a draft retention schedule but makes no mention to the aforementioned Scottish Council schedule.

The policy states that it will be reviewed every 3 years but is dated January 2003. The Service advised that arrangements were in place prior to the audit to review this policy.

Management Action Plan

a) The Information Compliance Manager will arrange for a revised Records Management Policy to be presented to the Strategic Policy & Resources Committee in December 2014 which will address the above issues, in that the revised policy will refer to the Council's information security standards and stipulate that the Council has adopted the Scottish Council on Archives Records Retention Schedule.

b) The Frequently Asked Questions on the Data Protection page of ***Eric*** will be amended to refer to the Scottish Council on Archives Records Retention Schedule.

Importance:	Medium
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	(a) and (b) December 2014
Required Evidence of Completion:	a) Updated Records Management Policy b) Updated FAQs on Eric

Auditor's Comments

Satisfactory

Action Point 5 - Scottish Government Guidance for Planning Authorities

Scottish Government data protection guidance for planning authorities from August 2013 states that there is a need for planning authorities to hold personal details such as names, addresses, telephone numbers and e-mail addresses. The guidance adds that such data is not relevant to the decision making process and there is no need for it to be published on websites.

The guidance further states authorities should be clear and open about how planning application information will be used. Applicants should be made aware of what information will be published on the internet and handling policies included in application forms with website guidance confirming that signatures and personal e-mail and telephone details will be redacted. The 'submitting a planning application' webpage or the hyperlinked planning application guidance notes fail to inform individuals that their data will be published. The householder application for planning permission also fails to inform individuals that personal data is published.

The 'making a representation' section on the PKC website, which concerns objections and comments of support, states information will be treated as public documents and displayed for public inspection with address details, signatures, personal telephone numbers and personal e-mail addresses undergoing redaction before being published. However, testing revealed that papers presented to the Local Review Body do not routinely redact objectors' addresses.

The August 2013 guidance also recommends that representations should be removed from websites when an unchallengeable decision on the application has been made. The Service has not yet established a routine to ensure that this is undertaken.

Management Action Plan

a) The Information Compliance Manager will liaise with the Development Quality Manager to agree the standardised wording for the data protection handling policy quoted on planning documentation.

b) The Information Compliance Manager will meet with the Development Quality Manager to agree a plan to ensure the publication and redaction of information relating to planning documentation is aligned to the Scottish Government data protection guidance of August 2013 and report the outcome to the SIRO.

Importance:	High
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive's Service

Date for Completion (Month / Year):	a) December 2014 b) December 2014.
Required Evidence of Completion:	a) Data protection handling policy b) Agreed plan /report to SIRO

Auditor's Comments

Satisfactory

Action Point 6 - Data Protection Registration Entry

The data protection policy requires an annual return from Services on the use and processing of personal information within their Service and that Services inform the data protection officer of any amendments to the data protection register entry as and when they occur.

The data protection officer was unable to provide evidence that this had occurred but advised that the registration is checked to ensure that it is correct and that, given the nature of the Council's business activity, the registration was unlikely to change.

The failure to retain annual returns from Services regarding the use and processing of personal information or any updates and amendments relating to the register entry makes it difficult to evidence adherence with the requirements of the policy.

Management Action Plan

The Information Compliance Manager will ensure that adequate annual returns are received from Services regarding the use and processing of personal information within their Service. These returns will be recorded in line with the requirements of the data protection policy.

Importance:	Low
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive's Service
Date for Completion (Month / Year):	January 2015
Required Evidence of Completion:	Copy of an annual DP return from a Service

Auditor's Comments

Satisfactory

Action Point 7 - Data Sharing

The data protection policy states that individuals will be informed at the point of data capture of “The identity of any organisation other than the Council with whom the information may be shared”.

Audit testing revealed that in the course of their duties Council staff may share information with external bodies such as the Child Support Agency and the Police. However, forms used at the data capture stage, such as the liability for council tax form, do not specifically comply with the above policy as the wording used does not specifically name the identity of any organisation with whom information may be shared, but states that disclosures to third parties will only be made to agents employed by the Council to recover unpaid debts and those organisations with legal right of access e.g. Inland Revenue.

The Information Compliance Manager advised the wording on the council tax form was in order and that, for clarity, the wording of the data protection policy would benefit from review.

Management Action Plan

The Information Compliance Manager will review and amend the data protection policy sharing of data wording.

Importance:	Low
Responsible Officer:	D Henderson, Information Compliance Manager
Lead Service:	Chief Executive’s Service
Date for Completion (Month / Year):	March 2015
Required Evidence of Completion:	Updated data protection policy

Auditor’s Comments

Satisfactory