INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Information Systems Policies
TO:	Deputy Chief Executive (AJ)	**DATE:**	25 October 2019
C.C.	Chief Executive Head of Finance Democratic Services Manager Information Governance Manager ICT Services Manager Portfolio Holder – Cllr Day		

---

1 Introduction

1.1 In accordance with the Audit Plan for 2019/20 an audit review of the Council's information system policies was completed in September 2019. This report presents the findings and conclusions drawn from the audit for information and action where appropriate.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and co-operation received during the audit.

2 Background

2.1 This audit was undertaken to review the existence and adequacy of the Council's information systems policies.

3 Scope and Objectives of the Audit

3.1 The audit was designed to assess and provide assurance on the following key areas:

- Policy framework for data protection, records management, information security and data sharing
- Information security policy
- Policies are published on the Council's intranet
- All policies follow an agreed format and styling
- New and existing policies are subject to regular review
- Information systems technical build standards.

3.2 Testing was performed to confirm that controls identified have operated as expected with documentary evidence being obtained where possible, although some reliance has had to be placed on verbal discussions with relevant staff.

4 Findings

4.1 Recommendations from Previous Report

4.1.1 This section is not applicable as this the first audit of this area.

4.2 Policy framework

4.2.1 An understanding of the policies in place for the management of information systems was obtained through discussion with ICT management during the audit. An information security and governance policy framework incorporating key elements including data protection, records management, information security and data sharing was found to be in place at the Council.

4.2.2 Key policies making up the framework were identified and obtained during the review. These were used in the process of reviewing the adequacy of the policies in in operation at the Council and key findings are detailed below.

4.3 Information security policy

4.3.1 The high level 'Information Security and Conduct Policy' describes the overall approach to information security and details a number of sub-policies that make up the framework. This policy, and sub-policies, documents the controls and processes in place to ensure that information is appropriately secured against issues arising that impact the confidentiality, integrity, and availability of Council data.

4.3.2 This policy was reviewed and found to document and define key information security roles and responsibilities, the Council's approach to maintaining the security and confidentiality of information, and includes references to all relevant sub-policies.

4.3.3 A sample of sub-policies was selected and reviewed for completeness and adequacy. This identified that the 'Information Security Incident Reporting' policy is in need of updating to reflect changes to requirements around the reporting of security incidents introduced as a result of GDPR. The policy currently states, for example, that there is "*no legal obligation in the Data Protection Act to report losses*" to the ICO, and makes no reference to the 72-hour timescale introduced as part of GDPR.

Risk

There may be a potential breach of GDPR requirements regarding incident reporting.

Recommendation

The 'Information Security Incident Reporting' policy should be reviewed and updated.

4.4 Information Governance Policies

4.4.1 It was noted in discussion with management that an exercise to review and update information governance policies and procedures was ongoing at the

time of audit and that work was required to substantially update policies covering data retention, data handling and classification of data in particular.

Risk

There may be ineffective information governance processes and controls in the absence of documented policies.

Recommendation

Ongoing work to update data retention, data handling and classification policies should be completed and updated policies should be made available to staff.

4.4.2 It was noted during testing that there has not historically been a process in place to ensure that data retention schedules are regularly reviewed and updated. As information asset owners have recently been assigned to all information assets it is recommended that an exercise to review retention schedules to sure they remain valid is undertaken and that this is repeated on an annual basis.

Risk

Data may be held longer than required and/or disposed of in breach of legal requirements.

Recommendation

Data retention schedules should be brought up to date and a regular review process should be introduced.

4.5 **Policies are published on the Council's intranet site**

4.5.1 Information system security and governance policies tested as part of this audit were found to be made available on the Council's intranet site.

4.5.2 Key information governance policies including the Information Governance Management Framework, Data Protection and Privacy Policy, Information and Access Rights, Records Management Policy, Information Security Incident Management Policy are also published on the external-facing Council website.

4.6 **Agreed format and styling**

4.6.1 Policies reviewed during the audit were found to follow a standard template, with some minor exceptions. The policy template includes: a revision and version history section listing the dates of review and detail of any changes made; a section covering policy governance requirements including detailing the person(s) responsible for developing and implementing the policy and the person ultimately accountable; the required distribution of the policy; and any relevant references to other Council policies or legislation.

4.7 **Regular review of policies and procedures**

4.7.1 There is a Council requirement that all policies should be reviewed on an at-least annual basis. Testing was undertaken to determine the date of last review for key policies reviewed during the audit.

4.7.2 Testing identified that, in the majority of cases, policies are reviewed and updated frequently in accordance with Council policy and that the documents revision history is updated to reflect the changes made.

4.7.3 It was noted, however, that a number of key information governance polices are overdue for updating having last been reviewed on dates ranging from February – April 2018. It is understood from discussion with management that this is due to the significant amount of work and changes to policies and procedures required as a result of GDPR and that work on bringing these up-to-date is underway.

Risk

There may be an impact to systems / services in the event of incorrect procedures being followed in the absence of up-to-date policies.

Recommendation

All remaining policies should be reviewed and updated.

4.8 **Information systems technical build standards.**

4.8.1 The Council's approach to build standards is documented as part of the 'ICT Services System Lockdown Policy'.

4.8.2 The policy includes the requirement that a standard build process should be used for all Council desktop computers in order to minimise the risk of damage to the network due to the lack of security software, ensure a standard environment to aid software deployment, and help ensure software licensing compliance. This process is monitored by the use of a checklist each time a desktop or 'thin client' is built. A similar checklist was found to be in place for virtual servers.

4.9 **Record of processing activities**

4.9.1 GDPR requirements state that organisations must "*maintain a record of processing activities under its responsibility*" and define the minimum criteria that must be recorded in relation to the data held.

4.9.2 Testing identified that the Council is currently working on a comprehensive record of processing activities. Although a record of processing activity spreadsheet is currently in place for each Council department, it is noted that these are at varying degrees of completion, with some containing missing data.

4.9.3 While individual service areas have a responsibility to review and update this record on a regular basis, it is recommended that a regular oversight exercise be undertaken to ensure the record of processing activity is kept up to date. An exercise to audit a sample of departments from across the Council to review the completeness and accuracy of this data is also recommended.

Risk

There may be a breach of GDPR requirements regarding the need to demonstrate compliance.
Recommendation

An exercise to review the accuracy and completeness of the Council's record of processing activities should be undertaken on a regular basis to ensure the record is up to date. Management should also consider audits of individual departments to verify the accuracy of data in the record.

5 Conclusions

5.1 The audit did not highlight any urgent issues materially impacting the Council's ability to achieve its objectives. The audit did, however, identify five Medium rated issues which, if addressed, would improve the overall control environment.

As a result, the findings are considered to give MODERATE assurance around the management of information systems policies.

5.1 The assurance bands are shown below:

Level of Assurance	Definition
Substantial Assurance	There is a sound system of control in place and compliance with the key controls.
Moderate Assurance	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited Assurance	The system of control is generally weak and there is non-compliance with controls that do exist.

6 Management Action

6.1 The recommendations arising above, are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of Information Systems Policies – October 2019

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.3.3	The 'Information Security Incident Reporting' policy should be reviewed and updated.	There may be a potential breach of GDPR requirements regarding incident reporting.	Medium	Information Governance Manager	The policy is already under review with target completion date (for adoption) of December 2019.	23 Dec 2019

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.1	Ongoing work to update data retention, data handling and classification policies should be completed and updated policies should be made available to staff.	There may be ineffective processes in the absence of documented policies.	Medium	Information Governance Manager	The polices are already under review with target completion date (for adoption) of December 2019.	23 Dec 2019

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.4.2	Data retention schedules should be brought up to date and a regular review process should be introduced.	Data may be held longer than required and/or disposed of in breach of legal requirements.	Medium	Information Governance Manager	This is not the responsibility of the IG Manager but the relevant service areas. However, the IG Manager is in the process of working with all Teams (within departments to remind them about these and to bring them up to date).	Not applicable.
4.7.3	All remaining policies should be reviewed and updated.	There may be an impact to systems / services in the event of incorrect procedures being followed in the absence of up-to-date policies.	Medium	Information Governance Manager	The polices are already under review with target completion date (for adoption) of December 2019.	23 Dec 2019

Report Ref.	Recommendation	Risk	Risk Rating*	Responsible Officer(s)	Management Response	Target Date
4.9.3	An exercise to review the accuracy and completeness of the Council's record of processing activities should be undertaken on a regular basis to ensure the record is up to date. Management should also consider audits of individual departments to verify the accuracy of data in the record.	There may be a breach of GDPR requirements regarding the need to demonstrate compliance.	Medium	Information Governance Manager	The IG Manager has been meeting with teams within Service Areas as in parallel to the retention schedules. However, part of this action should be for all Heads of Services (as Data Asset Owners) to ensure these records are correct. Also, both this and retention schedule should be an area that Audit test as part of their routine audits of each service area to validate the processes.	Not applicable.

* Risk Ratings are defined as follows:

High Risk: Issue of significant importance requiring urgent attention.
Medium Risk: Issue of moderate importance requiring prompt attention.
Low Risk: Issue of minor importance requiring attention.