

AUDIT COMMITTEE

17 JULY 2014

INFORMATION GOVERNANCE POLICIES

Report from: Perry Holmes, Assistant Director, Legal & Corporate Services,
Monitoring Officer

Author: Perry Holmes, Assistant Director, Legal & Corporate Services,
Monitoring Officer

Summary

This report is to seek formal approval of the policies and guidance first presented to the Audit Committee on the 11 July 2013.

The suite of Information Governance policies and guidance are set out within Supplementary Agenda No.1.

1. Budget and Policy Framework

1.1 It is within the ambit of the Audit Committee to consider the area of information governance.

2. Background

2.1 The Council as a “public authority” and as a holder of personal and general information is subject to a number of well-known pieces of legislation. For example, individuals are entitled to ask to see the information we hold about them under the Data Protection Act. Individuals can seek to access general information about council processes and decisions under the Freedom of Information Act. Under the less well known Environmental Information Regulations there are access rights to a specific set of non-personal information.

2.2 The suite of Information Governance policies and guidance set out below were first presented to the audit committee in July 2013 with a view that the policies would go out to consultation and be “road tested”.

- Information governance policy
- Data breach policy and guidance
- Data protection policy
- Data protection guidance

- Environmental information policy
- Environmental information guidance
- Freedom of information policy
- Freedom of information guidance
- Protective marking policy
- Records management policy.

2.3 The consultation with officers has concluded.

2.4 The policies and guidance has been revised with some changes, which are detailed on the "*Document control*" section of each policy.

3. Advice and analysis

3.1 Ensuring that the Council has a set of sound up to date policies and guidance for officers to use is part of ensuring good information governance.

3.2 The Information Commissioner's Office has oversight of data protection and freedom of information and has powers to prosecute public authorities and to impose substantial fines. In June 2013, Glasgow City Council was fined £150,000.00 for the loss of two unencrypted laptops containing the personal data of 20,000 people. In October 2013, North East Lincolnshire was fined £80,000 for the loss of an unencrypted memory stick containing personal data of 300 special needs pupils. Councils need to ensure that they have appropriate organisational safeguards in place to protect the security of personal data. This includes guidance and support available to officers who deal with personal data and other information on a day-to-day basis.

3.3 The suite of information governance policies and guidance were uploaded to the Intranet for officers to access. The guidance follows a self-help model with Officers seeking advice and support from Legal Services only where necessary.

4. Consultation

4.1 Consultation on the proposed changes has taken place involving the Security and Information Governance Group chaired by the Assistant Director of Legal & Corporate Services, senior managers and the Caldecott Guardian.

5. Risk management

- 5.1 There are reputational, legal and financial risks to the Council for not pro-actively seeking to ensure appropriate information security and governance.

Risk	Description	Action to avoid or mitigate risk
Reputational, legal and financial	A data breach occurs leading to the council being prosecuted by the Information Commissioner and fined	Refresh and augment the policy and guidance information available to Service Managers. Provide training to Managers and officers.
Financial	The Information Commissioner has imposed monetary fines on Councils for data breaches. If the Council stores both electronic data and papers records longer than necessary it incurs associated storage and energy costs unnecessarily.	The Security and Information Governance Group promotes good house-keeping of information and records.

6. Financial and legal implications

- 6.1 The financial and legal implications are set out in the body of the report.

7. Recommendation

- 7.1 The Audit Committee is asked to approve the suite of Information Governance policies and guidance.
- 7.2 The Audit Committee is recommended to delegate authority to the Assistant Director, Legal & Corporate Services, Monitoring Officer to amend the suite of Information Governance policies and guidance in compliance with current legislation and good practice.

Lead officer contact

Perry Holmes, Assistant Director, Legal & Corporate Services

Background papers

None.