Information Governance Policy

May 2018

1. INTRODUCTION

1.1 Information is a valuable asset that the Council has a duty and responsibility to protect. This responsibility is placed on the Council by the Data Protection Bill 2018 and EU General Data Protection Regulations (GDPR) monitored and regulated by the Information Commissioner's Office and the Local Public Services Data Handling Guidelines.

1.2 The Information Commissioner's Office now has powers to enable them to impose monetary penalty notices on organisations for up to €20,000,000 or 4% of annual turnover (depending on which is larger) for breaches of the Data Protection Act 2018 and EU General Data Protection Regulations (GDPR) along with having the authority to carry out assessments of organisations to ensure their processes follow good practice.

1.3 The key guidance document that the Council would be measured against is the Local Public Services Data Handling Guidelines Version 4 produced in February 2017 by the Public Services Network in partnership with the Local Chief Information Officer Council, Society of Information Technology Management (Socitm), the Cabinet Office and the National Local Authority Warning, Advice and Reporting Point (NLAWARP). The Council therefore has an obligation to comply with these guidelines, to ensure good practice is being followed.

1.4 To ensure that information assets and information systems are used and managed effectively, efficiently and ethically, the Council has produced an Information Charter (see Appendix 1), this will work alongside the Information Governance Framework, to ensure everyone is aware of their obligations.

2. PURPOSE OF POLICY STATEMENT

2.1 The purpose and objective of this Information Governance Policy is to protect the Council's information assets from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage and maximise return on investments and business opportunities.

2.2 The Council is committed to protecting information through preserving;

Confidentiality: Protecting information from unauthorised access, use and disclosure from unathorised individuals, entities or processes.

Integrity: Safeguarding the accuracy and completeness of information assets. This may include the ability to prove that an action or event has taken place so that it cannot be repudiated later.

Availability: Being accessible and usable on demand by an authorised individual, entity or process.

3. INFORMATION GOVERNANCE FRAMEWORK

3.1 This Information Governance Policy is the over-arching document of the Council's Information Governance Framework, (see figure 1 below). The Information Governance Framework comprises of the Information Governance Policy and specific supporting procedures, standards and guidelines as follows:-

- Information Governance Policy and Information Governance Conduct Policy;
- ICT Security Policy;
- Email, Communications and Internet Acceptable Use Policy;

- Social Media Responsible Conduct Policy;
- Data Protection Impact Assessment;
- Removable Media Protocol;
- Mobile and Remote Working Protocol;
- Retention and Disposal ;
- Access and Security Protocol;
- Incident Reporting Procedure;
- Secure/Clear Desk Procedure;
- Subject Access Request Guidance
- Information Asset Registers
- Golden Rules
- Information Governance Managers Checklist
- Information Sharing Protocol

3.2 Figure 1 – Information Governance Framework

4. SCOPE

4.1 The Information Governance Policy, along with the Conduct Policy and all supporting documents, apply to all employees, Members of the Council, temporary staff, contractual third parties, partners or agents of the Council who have access to any information systems or information for council purposes.

4.2 This Information Governance Policy applies to information in all forms including, but not limited to:-

- Hard copy or documents printed or written on paper;
- Information or data stored electronically, including scanned images;
- Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
- Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
- Information stored on portable computing devices including mobile telephones, PDA's and laptops;
- Speech, voice recordings and verbal communications, including voicemail; and
- Published web content, for example intranet and internet.

5. INFORMATION GOVERNANCE

5.1 Information Governance is the overall process of analysing, evaluating, assessing and mitigating the impact of risks to an organisation's information and information systems. Information Governance includes physical, personnel and information security and is an essential enabler towards making the Council work efficiently. Information risks must be managed effectively, collectively and proportionately, to achieve a secure and confident working environment.

5.2 The Council is aware that risks can never be eliminated fully and it has in place a strategy that provides a structured, systematic and focused approach to managing risk. However risk management is not about being 'risk averse', it is about being 'risk aware'. Some amount of risk taking is inevitable and necessary if the Council is to achieve its objectives. The Council seeks to capitalise on opportunities and to achieve objectives once those decisions are made. By being 'risk aware', the Council is in a better position to avoid threats, take advantage of opportunities and ensure its objectives and goals are realised.

5.3 Information risk will be managed by assigning roles and responsibilities and co-ordinating the implementation of this policy and all supporting documentation. Together these measures form the Information Governance lifecycle and will apply across the Council and in its dealings with all partners and third parties.

6. RESPONSIBILITY FOR INFORMATION GOVERNANCE

6.1 Senior Management (Directors, Assistant Directors and Service Unit Managers) has the responsibility and accountability for managing the risks within their own work areas. Employees have a duty to work safely, avoid unnecessary waste of resources and contribute to Governance initiatives in their own area of activities. The cooperation and commitment of all employees is required to ensure that Council resources are not squandered as a result of uncontrolled risks.

6.2 The Local Public Services Data Handling Guidelines 2017 and EU General Data Protection Regulations (GDPR) specify roles organisations must appoint to in relation to Information Governance as follows:-

- Data Protection Officer
- Accounting Officer
- Senior Information Risk Owner
- Information Asset Owners

6.3 These specific roles together with the Information Governance Group and Information Champions will work together with senior management to ensure compliance with best practice with the over-riding objective to keep the Council's information safe.

6.4 Table 1 below details the roles and responsibilities allocated to key staff.

Data Protection Officer	The **Data Protection Officer** has the formal responsibility for regulating and approving the application of information legislation for the organisation. **(To be determined)**
Accounting Officer	The **Accounting Officer** has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. **(Assistant Executive Director of Finance)**
SIRO	The **Senior Information Risk Owner** is familiar with and takes ownership of the organisation's information governance policy and strategy. **(Head of Risk Management and Audit Services)**
IAO	**Information Asset Owners** are Directors/ADs involved in running the relevant Directorate. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets.
SIAO	**Supporting Information Asset Owners** are at Service Unit Level and may have more familiarity with the information assets of that particular area. They are required to feedback to IAO's on what information their service area holds and how it is being managed.
System Owners	**System Owners** are responsible for Information systems. They will ensure system protocols are followed. They have responsibility to recognise actual or potential security incidents, consult their IAO on incident management, and ensure that information systems are accurate and up to date.
Information Champions	**Information Champions** are senior managers representing services from across each directorate and act as the liaison between the Information Governance Group and staff to ensure the framework, communications and training are effective and reach all staff