Information Management

- **Introduction**
- **Scope**
- **The Policy**
  - Key Messages
  - Risks
  - Policy Detail
  - Responsibilities

- **Policy Compliance**
  - Document Control

Appendix1 – Information Asset Owners for the Council

Introduction

This policy forms part of the Corporate Information Governance Group policy framework. It supercedes all previous policies on this subject matter.

Scope

This Policy applies to, but is not limited to, all of the councils, Councillors, Employees, Partners, contractual third parties and agents of the councils.

Information Management

Key Messages

The aim of this policy is to establish an effective governance structure to ensure that the council takes information management seriously and all staff understand their responsibility to handle all data in line with this policy.

The councils have a duty of care for the information they process. There are legal responsibilities under the 1998 Data Protection Act as set out in the eight Data Protection Principles. In particular, the seventh principle refers to the council's responsibility in protecting personal data as follows:

'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'

Risks

Consequences of poor information management or noncompliance with legislation may result in;

- Loss of Business and Efficiency.
- Reputational Damage.
- Financial Penalties.
- Damage to Integrity of information.

Policy Detail

This policy is intended to ensure:-

- Confidentiality is maintained and information is kept safe and secure
- Integrity is maintained and information remains accurate and unaltered
- Availability is maintained and information is available to be accessed by authorised users.

Responsibilities

- **Corporate Information Governance Group**

To advise each authority's SIRO, to review and update the information and security policies for the three authorities, to effectively manage information and security risks and to monitor and report via the SIROs any security breaches.

- **Senior Information Risk Owner**

The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the organisation and advises on the effectiveness of information risk management across the organisation.

- **Information Asset Owners**

The Information Asset Owner, who should be a system user of appropriate seniority, must ensure that:-

1. Information is being lawfully processed.
2. Access controls are in place, which are appropriate to the sensitivity of the information used by the system.
3. The major risks which may threaten the Confidentiality, Integrity and Availability of the information are identified and, where possible, mitigated;
4. Instances of misuse or abuse of the system are reported as per the Information Incident Reporting Policy.
5. The integrity of information is verified.

- **Staff**

All staff are personally responsible for securely handling any information that is entrusted to them in line with legislative and business requirements.

All staff should undertake data protection training to understand their responsibilities.

All staff will be an information asset owner for anything held on their individual electronic files in their personal area on the system (i.e. 'g' drive).

Information Asset Register

An information asset is any data that is organised and managed as a single entity.

This could be held on paper or in a computerised system.

- Each organisation will establish a register of all their information assets.
- The SIRO will ensure the information asset register is reviewed annually.

Protective Marking and Classification

The information that is created or processed by the councils is classed as OFFICIAL under the Government Security Classifications Policy. Therefore there is no requirement to protectively mark anything as OFFICIAL information.

There will be examples of information which is not disclosable for legislative reasons e.g. Local Government Act, Data Protection Act, and The Freedom of Information Act and some sensitive personal financial information.

You can, when sharing information, include a handling requirement such as “Do not distribute” or “Commercially Sensitive”.

Policy Compliance

If any person or organisation in scope is found to have breached this policy one of the following consequences may be followed:-

- Councils' disciplinary procedure.
- Breach of contract.
- Member code of conduct.

If you do not understand the implications of this policy or how it may apply to you, seek advice from your line manager or Senior Information Risk Officer.

Document Control		
Title/Version	-	Information Management Policy
Owner	-	Corporate Information Governance Group
Date Approved	-	
Review Date	-	
Reviewer	-	CIGG

Revision History			
Revision Date	**Reviewer (s)**	**Version**	**Description of Revision**
15/10/2015	Dave Randall Sophie Chadwick Will Causton Matthew Archer Hannah Lynch Clare Grant	1.0	First Draft for Consideration
23/09/2016	CIGG	1.1	Final Review

Appendix One

Information Asset Owners for the Council