# Information Risk Policy

## Document Control

| | |
|---|---|
| **Organisation** | Shropshire Council |
| **Title** | Information Risk Policy |
| **Author** | Roy Morris |
| **Filename** | Information Risk Policy - Final v1-0.doc |
| **Owner** | Information Governance Officer |
| **Subject** | Governance of Council information assets |
| **Protective Marking** | Not Protectively Marked |
| **Review date** | [to be inserted] |

## Revision History

| Revision Date | Revisor | Previous Version | Description of Revision |
|---|---|---|---|
| 14/6/2011 | Roy Morris | Draft 0.1 | Initial draft. |
| 4/7/2011 | Roy Morris | Draft 0.2 | Comments from IG Technical Sub-group and Risk Management & Insurance |
| 3/5/2012 | Roy Morris | Final 1.0 | Minor SIRO comments. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Document Approvals

This document requires the following approvals:

| Sponsor Approval | Date |
|---|---|
| Information Governance Group | 5/10/2011 |
| Senior Management Board | |
| Cabinet | |

## Document Distribution

This document will be added to the Corporate intranet. Staff will be informed by periodic staff notices and induction information.

**Contents**

## 1 Policy Statement

Shropshire Council will ensure that all Council information assets, including those provided by citizens and partners, are used, managed and protected effectively.

The Information Risk Policy supports the Corporate Information Security, Data Protection and Records Management Policies.

## 2 Purpose

The information we hold is an asset. If we use it well it provides many opportunities as it helps to make our business more efficient and improves the services we offer to the public. The risks in handling information are not only in failing to protect it properly, but also in not using it for the public good. Managing information opportunities and risk is about taking a proportionate approach so that both these aims are achieved.

The Council is committed to making the best use of the information it holds to provide efficient services to the public, whilst ensuring that adequate safeguards are in place to keep information secure and to protect the right of the individual to privacy.

## 3 Scope

This Information Risk Policy applies to all Shropshire Councillors, Committees, business partners, employees of the Council, contract or agency staff, volunteers and others with access to Council information and information systems.

Information security in schools is not within the scope of this policy.

## 4 Definition

This policy should be applied to all information or information systems used by the Council. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape, video or other media.
- Speech.

## 5 Risks

Shropshire Council recognises that there are risks associated with users accessing and handling information in order to conduct official Council business.

This policy aims to mitigate the following risks:

- Breach of legislation.
- Loss of information.
- Inappropriate access to or disclosure of information.
- Hindrance to or loss of information assets or facilities.

- Non-reporting of information risks/incidents.
- Loss of reputation should information be wrongly disclosed

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers**.**

## 6 Applying the Policy

To provide an effective information risk framework the Council will focus on four areas:

- People.
- Places.
- Processes.
- Procedures.

Information risk processes should complement the existing Corporate Risk Management Framework and provide input into overall risk management plans.

### 6.1 People

The Council will develop a culture that properly values, protects and uses information for the public good. Information is a key business asset and is not simply an IT issue. Clear lines of accountability for information assets will be established throughout the Council together with a programme of staff awareness raising, starting at induction, but continually updated, setting out the expectations of staff.

Responsibilities:

**Elected Members and Senior Management Board**

- The Council and its Members, will actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment and acknowledgment of information security responsibilities.

**Audit Committee**

- The Audit Committee has overall responsibility for ensuring that information risks are assessed and mitigated to an acceptable level. Information risks should be handled in a similar manner to other strategic risks such as financial, legal and reputational risks.

**Senior Information Risk Owner (SIRO)**

- The Corporate Head of Legal & Democratic Services is the Council's nominated SIRO. They have responsibility for providing a written judgement of the security and use of the business assets at least annually to support the audit process and provide advice on the content of their Annual Governance Statement.
- Act as advocate for information risk on the Senior Management Board.
- Chair the Information Governance Group (IGG).

**Information Governance Group**

To formulate policy, strategy, standards and guidance to support the effective and efficient use of Council information, whilst complying with legislation, Regulations, Government requirements and adopted best practice.

Chaired by the SIRO, membership: Corporate Heads, Group Managers, Head of Audit Services, Information Governance Officer (Area Directors, attendance as required).

**Area Directors/Heads of/Group Managers**

- To have procedures in place to ensure all existing, new and temporary staff and contractors have read and understood their obligations to comply with this Policy and supporting standards when using Council information.
- To ensure information processed within their Service Area complies with the Policy and supporting standards.
- To ensure Privacy Impact Assessments are conducted when making service and system changes.
- To provide assurance to the SIRO on the security and use of information assets within their remit.
- To raise any risks which may arise in their Service Area.

**Information Asset Owners (IAO)**

- Information Asset Owners are individuals involved in running the relevant service area with responsibility for understanding and addressing risks to the information assets they 'own'.
- They provide assurance to the Group Manager on the security and use of these assets.

**Information Asset Administrators (IAA)**

- Operational staff with the day to day responsibility for managing risks to their information assets.

**Line Managers**

- To ensure staff adhere to the Policy and Standards in day to day operations.

**Staff**

- To comply with associated Policy and Standards and seek guidance from Line Managers or the Information Governance Team when necessary.

**Contractors/Suppliers, agency staff, partners and third-parties**

- To comply with the Policy and Standards and seek guidance from Information Asset Owners or the Information Governance Team when necessary.

**Information Governance Officer – (post in place)**
(in support of legislative requirements for Data Protection, Freedom of Information and Government Security Requirements)

- Lead on information governance issues across the Council.
- Development of information security policy, standards and procedures in conjunction with the Information Governance Group.
- Manage compliance of the Policy and supporting Standards.

- Record, manage and monitor information security incidents.
- To ensure appropriate training, guidance and support is made available to Members, staff and contractors.
- Ensure risk register is updated.

**Caldicott Guardian**

- The Corporate Director - People is the Council's nominated Caldicott Guardian. To provide an advisory role in relation to client information (Adult and Childrens' social care areas).

**Records Manager – (post in place)**
(in support of the Freedom of Information Code of Practice for Records Management requirements)

- Lead on records management issues across the Council
- Development of records management policy, standards and procedures in conjunction with the Information Governance Group.
- To ensure appropriate training, guidance and support is made available to Members, staff and contractors

**Internal Audit and External Assessors**

- Review and report against compliance of the Policy and Standards.

### 6.2 Places

The Council should ensure the security of its information through the physical security of our buildings, premises and systems. Regular assessments of information risks should be undertaken for discussion at the Information Governance Group.

### 6.3 Processes

The Council should check that proper document systems are in place and that our suppliers, contractors and partners work to the same standards when handling our information. The Council will monitor the effectiveness of our policies and standards and where appropriate, engage independent experts to test systems and services and make recommendations.

### 6.4 Procedures

The Council will produce and maintain standards and procedures supporting this policy and ensure mechanisms are in place to test, monitor and audit compliance against them.

### 6.5 Policy Framework

The Council will have in place supporting standards and procedures based around the following areas. These will be supplemented by additional operational or technical standards where required, refer to Appendix 1. Failure to comply with external standards may result in the cessation of access to data or external services, which will have an impact on the Council's ability to deliver public services.

**Asset Management**

- To achieve and maintain appropriate protection of organisational assets.
- All assets should be accounted for and have a nominated owner.

**Human Resources security**

- To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
- Access to information is modified promptly to reflect staff changes or departures.

**Physical and Environmental security**

- To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.

**Communications and Operations Management**

- To ensure the correct and secure operation of information processing facilities.

**Access Control**

- To ensure the correct and secure operation of information processing facilities.
- Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.

**Information Systems acquisition, development and maintenance**

- To ensure that security is an integral part of information systems.
- All security and privacy requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

**Information Security Incident Management**

- To ensure information breaches or security events are communicated in a manner allowing timely corrective action to be taken.

**Business Continuity Management**

- To counteract interruptions to business activities and to protect critical business processes from the effects of disasters or major failures of information systems and to ensure their timely resumption.

**Compliance**

- To avoid breaches of any law, statutory, regulatory or contractual obligations and of any security requirements.

**Risk and Privacy Impact Assessment**

- To identify and examine the potential risks to privacy, integrity and availability of the information when making changes to services or systems.
- To ensure a risk register is maintained and updated regularly which will identify those risks to which the Council are exposed as a direct result of the handling of data or exchange of information.

## 7 Policy Compliance

Staff found to be in breach of this procedure or the supporting documents may face disciplinary action. Any other person to whom this policy applies will be subject to appropriate action should its conditions be breached. This action may include withdrawal of rights of access to information or systems. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Information Governance team.

## 8 Policy Governance

Policy and Standards will be formulated by the Information Governance Group, with input from stakeholders as required.

Any changes to existing standards or procedures in support of this Policy will be considered by the Senior Management Board, under delegated powers.

It is responsibility of Elected Members, all Council staff, all temporary and agency staff and volunteers, accessing Council information or systems to ensure compliance with this Policy and supporting standards.

## 9 Review and Revision

This policy will be reviewed every 12 months.

Policy review will be undertaken by Information Governance Officer.

## 10 Appendix 1 - Supporting standards and legislation

The following standards should be in place to support this policy:

### 10.1 Internal

- Acceptable Use Standards (electronic services/equipment)
- Data Handling Standards
- Communications and Operation Management Standards.
- Government Connect (GCSx)/Public Services Network (PSN) Acceptable Usage Standards
- Human Resources Information Security Standards
- Security Incident Standards
- IT Access Standards
- IT Infrastructure Security Standards
- Remote Working Standards
- Removable Media Standards
- Software Standards
- Systems Development and Maintenance
- Protective Marking Standards
- Forensic readiness
- Social Media Standards
- Mobile device Standards
- Freedom of Information & Transparency Standards

### 10.2 External

The following list outlines key external standards that the Council should adhere to demonstrate that it processes information appropriately on behalf of citizens and partners.

**LGA Data Handling Guidelines for Local Government**
Standards to be adopted by Local Authorities to help engender public trust in the delivery of public services.

**NHS Statement of Compliance**
Annual assessment of processes used for handling data provided to the Council by the NHS.

**DWP Memorandum of Understanding**
Annual commitment to meet standards for the use of national DWP customer data for Revenues & Benefits services.

**Payment Card Industry (PCI) Standards**
Annual accreditation of manual and electronic processes used for electronic card payments.

**Government Connect Code of Connection/Public Services Network**
Attainment of annual external assessment to maintain connectivity to the Government's secure communications network (Government Connect).

**OGC Contract Rules**
Information security clauses to be inserted in Council contracts.

**ISO 27001**
International best practice standard.

**HMG Security Policy Framework**
To be adopted, where appropriate, when handling HMG assets or delivering services.

**Statutory Data Sharing Code of Practice**
Practice to be adopted for systematic or ad hoc sharing of personal data.

**Code of Recommended Practice for Local Authorities on Data Transparency**
To ensure transparency of Council data by publishing data to meet public demand in open formats and in a timely way.

### 10.3 Legislation

The following list outlines key information related legislation that the Council should adhere to demonstrate that it processes information appropriately on behalf of citizens and partners.

**Data Protection Act 1998**
Requirements to ensure legitimate processing of personal information and provision of an applicant's own personal information by responding to requests within statutory timescales.

**Freedom of Information Act 2000 (including Environmental Information Regulations 2004)**
Provide public access to disclosable information by publishing information in accordance with an adopted Publication Scheme and by responding to requests for information from members of the public within statutory timescales.

**The INSPIRE Regulations 2009**
Obligations on a local authority, or third-parties acting on their behalf, to publish 'spatial' datasets.

**Protection of Freedoms Act 2012**
Extension of Freedom of Information regulations and amendment of other information related regulations relevant to Council service delivery.