Information Risk Policy

DAVENTRY DISTRICT COUNCIL

Document control template

Organisation	*Daventry District Council*
Title	*Information Risk Policy*
Author	*Vikki Smith*
Filename	W:\Legal\B183 Data Protection\Information Risk\Information Risk Policy.rtf
Subject	*Information Governance*
Protective Marking	*Unclassified*
Review date	*January 2021*

Revision History

Version	**Revision Date**
0.1	*01/02/2013*
0.2	*23/01/2017*
0.3	*21/01/2019*

Contents

1 Policy Statement

Daventry District 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 Information Security and Incident Management Policy, Data Protection Policy, ICT Usage Practices and Information Handling Practices.

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 Daventry Councillors, Committees, employees, contract or agency staff, volunteers and others with access to Council information and information systems.

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

Daventry District 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.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council, reputational damage 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. An example information risk log is available in Appendix 2.

6.1 People

The Council will develop a culture that properly values, protects and uses information for the public good. Clear lines of accountability for information assets will be established throughout the Council together with a programme of employee awareness raising, starting at induction, but continually updated, setting out the expectations of employees.

Responsibilities:

Elected Members and Senior Management Team

- 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.

Corporate Governance Committee

- The Corporate Governance Committee has overall responsibility for ensuring that information risks are assessed and mitigated. 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 Resources Manager is the Council's nominated SIRO. He/she has responsibility for providing a written judgement of the security and use of the business assets at least annually to support the audit process. This judgement to be included in the Annual Governance Statement.
- Act as advocate for information risk on the Senior Management Team.

Service Managers/Information Asset Owners

- 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 Information Risk 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 act as Information Asset Owners (IAO) within their Service Area, with responsibility for

understanding and addressing risks to the information assets they 'own'.

- To provide assurance to the SIRO on the security and use of these assets annually. The SIRO will then inform SMT and Members through the Annual Governance Statement of any significant information risks.
- To determine employee level of access to information systems within their Service Area.
- To identify any information risks which may arise in their Service Area.

Line Managers

- To ensure all existing, new and temporary staff and contractors adhere to the Policy, Standards and Practices in day to day operations.
- To recognize their responsibilities with respect to the information held within their service area

Employees

- To comply with associated Policy, Standards and Practices and seek guidance from Line Managers or the Information Officer when necessary.

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

- To comply with the Policy, Standards and Practices and seek guidance from Information Asset Owners or the Information Officer when necessary.

IT Manager and Data Protection Officer –

(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
- 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, managers, employees and contractors.

Information Officer –

(in support of the Freedom of Information Code of Practice for Records Management requirements)

- Support with records management issues across the Council
- Development of information handling practices and procedures

Internal Audit and External Assessors

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

6.2 Places

The Council should ensure the security of its information through the physical security of our buildings, premises and systems.

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, practices 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, practices and procedures based around the following areas. These will be supplemented by additional operational or technical standards/practices where required - please 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 managers, 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 employee 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.

Information Risk 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

Employees found to be in breach of this policy 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 Officer.

8 Policy Governance

Any changes to existing standards and practices, or the introduction of new standards and practices, in support of this policy will be considered by the Senior Management Team and determined by the Chief Executive.

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

9 Review and Revision

This policy will be reviewed every 3 years. This will be undertaken by the Information Officer.

10 Appendix 1 - Supporting standards, practices and legislation

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

10.1 Internal

- ICT Usage Practices
- Information Handling Practices
- Government Connect (GCSx) Acceptable Usage Standards
- Employee Handbook – Code of Conduct for Employees
- Data Protection Policy and Manual
- Information Security Incident Management Policy and Procedure
- Media and Marketing Protocols
- Freedom of Information Guide to Information

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.

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

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).

UK Public Contract Regulations
Information security clauses to be inserted in Council contracts.

ISO 27001 – Information Security Management
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.

Local Government Transparency Code 2015
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.

General Data Protection Regulation and Data Protection Act 2018
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.

11 Appendix 2 – Example Information Risk Log

This document records identified risks to the service, their implications and actions taken to mitigate them. It should be updated at least monthly and copies saved with the file name including the date.
Read notes on "Defs and Notes" tab before use.

Identified Risks			Date		Initial Likelihood A to E	Initial Impact 1 to 4	Impact if Risk Occurs – Description	Risk status - R/A/G	Owner	Avoid/ Accept/ Reduce/ Transfer	Controls and Mitigation (Countermeasures)	Residual Likelihood A to E	Residual Impact 1 to 4	Risk status - R/A/G
Risk No.	Type: B/T/L	Description	Risk identified	Updated			(Consider – Health &Safety/ Cost/Time/Quality/ Environment/Reputation)							
1	B	Loss of information					Reputational damage - failure to meet statutory obligations. Possible financial penalties (up to £500,000) from the ICO if serious loss/misuse of personal data. Inability to provide necessary services to our customers.		Service Mgr/IOA	Reduce	Sufficient computer software with security measures in place. Properly trained officers. Business Continuity policies in place.			
2	B	Inappropriate access to or disclosure of information					Bad press, damaged reputation, loss of trust from customers, loss of business and for employees, the prospect of disciplinary action. Possible financial penalties (up to £500,000) from the ICO if serious loss/misuse of personal data		Service Mgr/IAO	Reduce	Access rights restricted to appropriately trained officers. Clear procedures in place.			
3	B	Hindrance to or loss of information assets or facilities					Reputational damage. Effect on the efficient operation of the Council. Inability to provide necessary services to our customers.		Service Mgr/IAO	Reduce	Adequate and trained officer. Sufficient computer software with security measures in place. Contingency policies in place and up-to-date.			
4	B	Non-reporting of information risks/incidents					Reputational damage.		Service Mgr/IAO	Reduce	Clear procedures in place. Adequate and trained officers, supported by up-to-date policies.			
5	B	Breach of legislation					Bad press, damaged reputation, loss of trust from customers, loss of business and for employees, the prospect of disciplinary action. Possible financial penalties (up to £500,000) from the ICO if serious loss/misuse of personal data		Service Mgr/IAO	Reduce	Adequate and trained officers, supported by up-to-date policies.			