Information Security Policy

1 Version History details and author

1.0 05/10/2010 Completed for distribution Jo White
1.0 27/10/2010 Approved by Information Governance Group Jo White
2.0 25/10/2011 Reviewed by Information Governance Group Jo White
3.0 27/03/2013 Reviewed by Information Governance Group. Document review dates amended. Jo White
4.0 27/09/2013 Reviewed by Information Governance Group. Section 4.5 added reference to security incidents informing ISMS improvements. Jo White
5.0 13/10/2014 Reviewed by Information Governance Group. Change to name of IGG Chair and rename the policy to Information Security Policy. Jo White
6.0 11/05/2015 Reviewed by Information Governance Group. Clarification of assets, continual improvement and update to standard. Jo White
7.0 09/08/2016 Reviewed by Information Governance Group. Jo White
8.0 09/10/2017 Reviewed by Information Governance Group. Transformation changed to ICT. GDPR added. IGG Chair changed. Jo White
9.0 03/12/2018 Reviewed by Information Governance Group. Assistant Director of ICT updated. Jo White
10.0 08/09/2020 Reviewed by Information Governance Group. Published documents dates updated. Jo White
11.0 11/05/2021 Reviewed by Information Governance Group. No changes. Jo White
12.0 02/11/2021 Reviewed by Information Governance Group. Website links and legislation updated. Jo White
13.0 07/02/2023 Reviewed by Information Governance Group. Agency workers and EIR added. Jo White

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control A.5.1.1 - Policies for information security
ISO Control A.5.1.2 - Review of the policies for information security
ISO Control A.6.1.1 - Information security roles and responsibilities
ISO Control A.18.1.1 - Identification of applicable legislation and contractual requirements

2 Introduction

Derbyshire County Council recognises that ICT systems and information are valuable assets which are essential in supporting the Council's strategic objectives. The Council recognises its obligations to protect information from internal and external threats and recognises that effective information security management is critical in order to ensure the successful enablement of ICT and delivery of business functions and services. The council is committed to preserving the confidentiality, integrity and availability of all physical and electronic assets.

Information security management is an ongoing cycle of activity aimed at continuous improvement in response to emerging and changing threats and vulnerabilities. It can be defined as the process of protecting information from unauthorised access, disclosure, modification or destruction and is vital for the protection of information and the Council's reputation.

This policy details Derbyshire County Council's approach to information security management and contains no sensitive or restricted information and may be freely publicised to relevant parties. A current version of this document is available to Council staff on the corporate intranet and is available to external parties on the Council's website at Importance of Information Security

The approach is based upon implementation guidance contained within ISO27002 - a code of practice for information security controls.

3 Scope

This Information Security Policy applies to all information assets as defined in the Council's Information Asset Management Policy including:

- ICT systems belonging to, or under the control of, Derbyshire County Council;
- Information stored, or in use, on Council ICT systems or in hard copy physical form;
- Information in transit across the Council's voice or data networks;
- Control of information leaving the Council;
- Information access resources;
- All parties who have access to, or use of ICT systems and information belonging to, or under the control of, Derbyshire County Council including:
    - Council employees
    - Elected Members
    - Third Parties
    - Temporary staff
    - Agency workers
    - Partner organisations, including Schools and Academies
    - Members of the public
    - Volunteers
    - Any other party utilising Council ICT resources

Application of this policy applies throughout the information lifecycle from acquisition / creation, through to utilisation, storage and disposal.

4 Responsibilities

Co-ordination: The Council co-ordinates information security management across the authority through an internal Information Governance framework chaired by the Director of Finance and ICT.

Security Officer: The Council's Information Security and Governance Manager is responsible for ensuring policies and procedures are in place to cover all aspects of ICT systems and Information security. All policies will be communicated across the Council to ensure good working practices and to minimise the risk to the Council's reputation.

Directors: are responsible for ensuring that ICT systems and information within their service areas are managed in accordance with the Council's Information Security Policy. Day to day responsibility for the management of ICT systems and information may be delegated to staff designated as information or system owners within departments.

Users of resources: It is the responsibility of any individual or organisation having access to the Council's ICT systems and information to comply with the Council's Information Security Policy, associated guidelines and procedures and to take adequate steps to safeguard the security of the ICT systems and information to which they have access. Any suspected or actual security weakness, threats, events or incidents must be immediately reported to the Information Security Manager via the Council's Incident Reporting procedure.

5 Policy Statement

The Information Security Policy is based on the ISO/IEC 27002:2013 implementation guidance for the British Standard for Information Security ISO/IEC 27001:2013 controls.
The Council is committed to the development and maintenance of an Information Security Management System based upon the International Standard the Council has developed this Information Security Policy to:

- Provide direction and support for information security in accordance with business requirements, regulations and legal requirements;
- State the responsibilities of staff, partners, contractors and any other individual or organisation having access to the Council's information assets.
- State management intent to support the goals and principles of security in line with business strategy and objectives.
- Provide a framework by which the confidentiality, integrity and availability of the Council's information assets can be maintained.
- Optimise the management of risks, by preventing and minimising the impact of Information Security incidents;
- Ensure that all breaches of information security are reported, investigated and appropriate action taken where required;
- Ensure that supporting ISMS policies and procedures are regularly reviewed and continual improvement is maintained to ensure progressive good working practices and procedures
- Ensure information security requirements are regularly communicated to all relevant parties.

5.1 Authorised Use

Access to ICT systems and Information for which the Council is responsible is permitted in support of the Council's areas of business or in connection with a service utilised by the Council. Authorised users are defined as: Council employees, elected members, authorised contractors, temporary staff, partner organisations or members of the public when using public information services provided by the Council.

5.2 Acceptable use

All users of ICT systems and information for which the Council is responsible must agree to, and abide by, the terms of the Council's ICT Acceptable Use Policy, associated security policies and applicable Codes of Connection or Conduct.

5.3 Security awareness

The Council is committed to promoting safe working practices. All employees will receive security awareness training commensurate with the classification of information and systems to which they have access. Staff working in specialised roles will receive appropriate training relevant to their role. Relevant information security policies, procedures and guidelines will be accessible and disseminated to all users. It remains the employees' responsibility to ensure they are adequately informed of information security policies and procedures.

5.4 Business Continuity

The Council has developed, and maintains, a Business Continuity Strategy based on specific risk assessment to maintain critical business functions in the event of any significant disruption to services or facilities on which the Council is reliant.

5.5 Monitoring and reporting

The Council reserves the right to monitor the use of ICT systems and information, including email and internet usage, to protect the confidentiality, integrity and availability of the Council's information assets and ensure compliance with the Council's policies. The Council may, at its discretion, or where required by law, report security incidents to the relevant UK authorities for further investigation. As part of the standard audit review process, Internal Audit will routinely assess compliance with the Council's Information Security Policy and applicable ISO27001:2013 controls and report matters to senior management or the Information Governance Group where appropriate. Security incidents reported through the Security Incident Management Policy and Procedures, will inform on the effectiveness of ISO27001:2013 controls and assist in identifying training and awareness requirements and improvements through the Corrective and Preventative Action (CAPA) procedure.

5.6 Risk Assessment

The Council has developed a Risk Management Strategy and the risk to the Council's ICT systems and information will be managed under this framework with reference to the guidelines detailed in *BS 7799-3:2006 Information security management systems – Part 3: Guidelines for information security risk management.* Reviews are independent, unbiased and verified by either internal audit or external parties when required.

5.7 Security Policy Review

The Council will conduct an annual review of the policy or following any significant security incidents, changes to UK or EU legislation or changes to the Council's business requirement or structure.

5.8 Asset Management

The Council will maintain an inventory consisting of all information assets which will be managed in accordance with the Council's information security policies and procedures.

5.9 Sanctions

Failure of Council employees to comply with the Council's Information Security Policy may lead to disciplinary action under the Council's disciplinary procedure.

Failure of contractors, temporary staff, public, partners or third party organisations to comply with the Council's Information Security Policy may result in termination of contracts and connections, suspension of services and/or lead to prosecution.

6 Compliance with legal and contractual obligations

Derbyshire County Council will abide by all UK legislation relating to information storage and processing including:

- The Data Protection Act (2018)
- UK General Data Protection Regulation (2018)
- The Freedom of Information Act (2000)
- The Environmental Information Regulations (2004)
- The Computer Misuse Act (1990)
- The Human Rights Act (1998)
- The Copyright, Designs and Patents Act (1988)
- The Regulation of Investigatory Powers Act (2000)
- The Electronic Communications Act (2000)
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended).

Derbyshire County Council will also comply with any contractual requirements, standards and principles required to maintain the business functions of the Council including:

- Protection of intellectual property rights
- Protection of the authority's records
- Compliance checking and audit procedures
- Prevention of facilities misuse
- Relevant codes of connection to third party networks and services

7 Development of specific information security policies, procedures and guidelines

The Council is committed to the ongoing development and review of information security policies, procedures and guidelines to manage the risk of emerging threats to its systems, services, information and data. This work will be co-ordinated by the Information Governance Group chaired by the Director of Finance and ICT. A list of current supporting documents is included in Appendices A-C. New policies,

procedures and guidelines are distributed to all stakeholders at the time of issue. Appendices A-C of this policy are updated during the annual Information Security review.

8 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies.
All Council employees, elected members, partner agencies, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council

The Council will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an individual then the matter may be dealt with under the disciplinary process.

Incident Reporting

Users will be continually made aware of and encouraged to use a page on the Council's staff website where they can report any breaches online or via a telephone call to the ICT Service Call Desk. Breaches can involve not only Information Technology equipment but also data that is mishandled, lost or abused or any other incident which may cause a security concern or which may contravene the Council's Safe Haven Guidance and associated policies.

Incident Management

During reporting of a breach, details of the incident will be entered into the call logging system - either by the person directly reporting the incident using the form on the staff website or by the Service Desk operator taking the call. Once the call has been entered into the system, an email is generated and sent to the Information Security Manager and also copied to the Assistant Director of ICT (Operations). The Information Security Manager will then determine if the incident needs to be escalated to the appropriate pre-identified departmental representative to deal with. Representatives looking into security breaches will be responsible for updating, amending and modifying the status and clearance code of incidents in the call logging system.

Appendix A

List of ISMS Security – Policies

Access Control – Review Date 31/03/2024
Access Control Policy for Volunteers – Review Date 31/03/2024
Applicable Legislation Register – Review Date 30/06/2023
Corporate Data Protection – Review Date 30/09/2023
Corporate Digital Records Preservation – Review Date 30/06/2023
Corporate Records Management – Review Date 31/08/2023
Corporate Scanning – Review Date 31/12/2023
Encryption & Cryptographic Controls – Review Date 31/03/2023
ICT Acceptable Use – Review Date 31/03/2023
Information Asset Management – Review Date 31/05/2023
Information Backup and Restore – Review Date 31/03/2024
Information Classification and Handling Policy – Review Date 31/01/2024
Information Security Management System – Review Date 30/11/2023
Information Systems Development and Maintenance – Review Date 30/04/2023
Acceptable Use of Internet, Email and Social Media – Review Date 30/04/2023
ISO27001 Scope – Review Date 31/08/2023
Mobile Device – Review Date 31/10/2023
Network Security- – Review Date 28/02/2024
Operational Management – Review Date 31/10/2023
Password – Review Date 31/10/2023
Premises Access Control – Review Date 31/12/2023
Public Internet Access – Review Date 31/05/2023
Records Disposal – Review Date 30/11/2023
Secure Work Place – Review Date 31/10/2023
Secure Email – Review Date 30/06/2023
Secure File Transfer – Review Date 31/03/2023
Server Security – Review Date 28/02/2024
Supplier Information Security – Review Date 31/05/2023
Surveillance Camera – Review Date 30/09/2023
Third Party Connection – Review Date 31/12/2023
Wireless Network – Review Date 30/11/2023

List of ISMS Security - Procedures

Confidential Waste – Review Date 31/03/2024
Corrective and Preventative Action – Review Date 31/01/2024
Corporate Subject Access Request – Review Date 30/09/2023
Data Protection and Storage Media Handling – Review Date 31/05/2023
Desktop and Mobile Device – Review Date 31/10/2023
Disaster Recovery / Business Continuity Management – Review Date 28/02/2023
Document and Record Control – Review Date 31/01/2024
ICT Security Awareness – Review Date 31/03/2023
Information Request – Review Date 31/08/2019
Malicious Software and Anti-Virus – Review Date 31/12/2023
Mobile Working – Review Date 31/07/2023
Physical and Environmental Infrastructure – Review Date 31/07/2023
Records Appraisal – Review Date 31/07/2023

Records Disposal – Review Date 30/11/2023
Secure Destruction of Optical and Magnetic Media – Review Date 31/05/2023
Security Incident Management – Review Date 30/11/2023

List of ISMS Security - Guidance notes

Guidance for the offsite storage of documents – Review Date 28/02/2024
Risk Assessment Guidance for DCC Risk Owners – Review Date 31/01/2023
Risk Treatment Guidance for DCC Risk Owners – Review Date 31/01/2023
Safe Haven – Review Date 31/01/2023