Information Governance
Information Security Policy

Version: 1.4.3
Published: 01 March 2018

Document Control

Related Documents

Title	Author	Version & Date

Revision History

Release Date	Revision Version	Summary of Changes
07/03/2012	V0.1	Reason for review
16/03/2012	V0.2	Creation
21/08/2012	V1.0	Amendment to responsibility section
20/11/2012	V1.1	Final for publication
18/09/2014	V1.2	Reformatted and corrected
12/05/2015	V1.3	Reviewed and updated
12/02/2016	V1.4	Reviewed and updated
12/05/2017	V1.4.1	Reviewed
01/09/2017	V1.4.2	Reviewed
01/03/2018	V1.4.3	DPO Responsibilities Para 6.6 updated

Reviewed By
This document (or component parts) has been reviewed by the following:

Post or Group Title	Revision Version	Approval Date
Information Security Manager	V1.2	18/09/2014
Information Security Officer	V1.3	12/05/2015
Information Security Officer	V1.4	12/05/2016
Information Security Officer	V1.4.1	12/05/2017
Information Security Officer	V1.4.2	01/09/2017
Information Security Officer	V1.4.3	01.03.2018

Document Approval
This document requires the following approvals:

Post or Group Title	Revision Version	Approval Date
Information Security Manager	V1.2	18/09/2014
Corporate Governance Group	V1.3	22/06/2015
Information Security Manager	V1.4	22/06/2016
Corporate Governance Group	V1.4	08/03/2017
Information Security Manager	V1.4.1	12/05/2017
Information Security Manager	V1.4.2	01/09/2017
Information Security Manager	V1.4.3	01/03/2018

Contents

1. INTRODUCTION 5
2. OBJECTIVE 5
3. SCOPE OF POLICY 5
4. POLICY 5
4.1. Legislation 6
5. DEFINITIONS 7
5.1. Information and data 7
5.2. Personal and Sensitive Information 7
6. RESPONSIBILITIES 8
6.1. Chief Executive 8
6.2. Senior Information Risk Owner (SIRO) 8
6.3. Information Governance Lead 8
6.4. Information Security Manager 8
6.5. Caldicott Guardian (Children's Services and Health and Care Services only) 9
6.6. Data Protection Officer Responsibilities 9
6.7. Corporate Directors / Line Managers 9
6.8. All Users 10
7. VALIDITY OF POLICY 10
8. AUDIT DETAILS 10
9. REFERENCES 10

1. INTRODUCTION

This document defines the Information Security Policy for Cumbria County Council (the council).

This Information Security Policy applies to Top Level Security within the scope of the Information Security Management System and covers the information, information systems, networks, physical environment and relevant people who support the business functions.

This document:

- Sets out the organisation's policy for the protection of the confidentiality, integrity and availability of its assets, that is hardware, software and information handled by information systems, networks and applications.
- Establishes the security responsibilities for information security.
- Provides reference to the documentation which comprises the Information Security Management System for the above scope.

It is therefore supported by other thematic policies and procedures dealing with specific functional areas and requirements (e.g. for working off site or encryption)

2. OBJECTIVE

The objective of this policy is to ensure the security of the council's information assets by implementing a suitable set of controls, (which could be policies, practices, procedures, organisational structures and software functions), which reflect and meet the business need, and which will achieve an assessable standard of compliance.

Information security is characterised here as the preservation of:

- ***Confidentiality*** – ensuring that information is accessible only to those authorised to have access
- ***Integrity*** – safeguarding the accuracy and completeness of information and processing methods
- ***Availability*** – ensuring that authorised users have access to information and associated assets when required.

3. SCOPE OF POLICY

This policy applies to all information systems, networks, applications, locations and users within the purview of the council.

4. POLICY

The council's overall Information Security Policy is described below:

Council information systems, applications and networks are available when needed, they can be accessed only by legitimate users and contain as complete and accurate information as is possible.

The information systems, applications and networks must also be able to withstand or recover from threats to their availability, integrity and confidentiality and be protected against accidental loss of data.

To satisfy this, the council will undertake to do the following:

- Protect all hardware, software and information assets under its control. This will be achieved through the implementation of a set of well-balanced technical and non-technical measures.

- Provide both effective and cost-effective protection that is commensurate with the risks to its assets.
- Implement the Information Security Management System (ISMS) in a consistent, timely and cost effective manner.

4.1. Legislation

The council is governed by the law of England and Wales. The following is a non-exhaustive list of legislation which is relevant to information security:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice)-(Interception of Communications) Regulations 2000
- Obscene Publications Act 1964
- Protection of Children Act 1999
- Criminal Justice Act 2003
- Copyright, Designs and Patents Act (1988)
- Computer Misuse Act (1990)
- Protection from Harassment Act 1997
- Sex Discrimination Act 1975
- Race Relations Act 1976

The Council will endeavour to comply with these and any other relevant laws and legislation.

Additionally, users are under a common law obligation to preserve the confidentiality of this information and to only use it for the purposes for which it was intended.

The council will:

- Carry out security risk assessment(s) in relation to all the business process covered by this policy which will:
    - cover all information systems, applications and networks that are used to support those business processes,
    - identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability of business critical applications and systems using a recognised business methodology,
    - produce System Security Policies for all major information systems, applications and networks. These policies should be developed on the basis of an analysis of risks and based on a standard template,
    - produce System Operating Procedures and ensure that all users of the system be made aware of the contents and implications of the relevant procedures,
    - provide security awareness training for all users to ensure that they are aware of their responsibilities for security, and the actions that they need to undertake in order to discharge those responsibilities,
    - ensure that all users of information systems, applications and the networks are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities and are aware that irresponsible or improper actions may result in disciplinary action,
    - ensure that contingency plans and disaster recovery plans are produced for all critical applications, systems and networks. The plans must be reviewed and tested on a regular basis,

- ensure that there is an effective configuration management system for all information systems, applications and networks,
- ensure that measures are in place to detect and protect information systems, applications and networks from viruses and other malicious software,
- ensure that all operational applications, systems and networks are monitored for potential security breaches where functionality allows and to apply penetration tests where appropriate,
- any suspect incident or weakness of security should be reported and investigated,
- ensure that all connections to external networks and systems have documented and approved System Security Policies,
- ensure that all third-party connections into the network and systems from outside have documented and approved System Security Policies,
- ensure that all information systems, applications and networks are reviewed by the Information Security Officer, before they commence operation, for compliance with Security Policy Guidelines,
- ensure that changes which may impact on the security of an information system, application or network are reviewed by the relevant project/system manager. All such changes must be reviewed and approved by the Information Security Manager,
- ensure that mobile device and content encryption policy and process is in place to meet recommended standards. If you are uncertain of the current recommendations, discuss with the Information Security Manager.

5. DEFINITIONS

5.1. Information and data

Information results from the collection and collation of data. Information can be held and used in many forms including (but not limited to) electronic records, paper (hard copy), phone calls, audio and video recordings and conversations. Throughout this policy information and data can be regarded as being the same thing.

5.2. Personal and Sensitive Information

The following list contains examples of personal and sensitive information (This list should not be considered exhaustive):

- Person Identifiable Data, e.g. name, postcode, driving licence number of a service user or employee
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations
- Politically sensitive information
- Information relating to security, investigations or proceedings
- Information provided in confidence
- Personal or sensitive information shared by other bodies such as NHS, central government or the police.

An easy way to identify whether information is personal or sensitive is to consider the following:

- Is the information covered by the Data Protection Act 1998?
- Could the release of the information cause problems or damage to individuals, the public, the council or a partner organisation?
- Could release of the information prejudice the outcome of negotiations or investigations?

If in doubt seek advice from line management or relevant Information Security personnel.

6. RESPONSIBILITIES

6.1. Chief Executive

The Chief Executive as Accounting Officer has delegated the overall security responsibility for security, policy and implementation to the Director designated as the Senior Information Risk Owner.

Responsibility for implementing this policy within the context of IT systems development and use in the organisation is delegated further to the Information Governance lead.

6.2. Senior Information Risk Owner (SIRO)

The council's SIRO lead is:

- Accountable for information risk
- Owns the overall information risk policies and procedures
- Fosters a culture for protecting and using data
- Will consider decisions made by the Corporate Governance Group and ratify those decisions as appropriate
- Will ensure that the Corporate Management Team is regularly and adequately briefed on information governance risk issues
- Provides a focal point for managing information risks and incidents
- Is concerned with the management of all information assets

6.3. Information Governance Lead

The council's designated Information Governance lead is responsible for:

- Ensuring that the council has appropriate information security policies in place
- Ensuring that the Information Security Manager provides the council with an appropriately qualified Security Officer service
- Ensuring that a Data Protection Officer is identified

6.4. Information Security Manager

The Information Security Manager is responsible for:

- Acting as a central point of contact on information security within the organisation, for both users and external organisations.
- Implementing an effective framework for the management of security.
- The formulation, provision and maintenance of Information Security Policies.
- Advising on the content and implementation of the Information Security Programme.
- Producing and supporting the production of organisational standards, procedures and guidance on Information Security matters for review by the SIRO, Section 151 Officer, Caldicott Guardian and other senior staff; for approval by the Corporate Governance Group, on behalf of the council Corporate Management Team.
- Co-ordinating information security activities particularly those related to shared information systems or IT infrastructures.
- Liaising with external organisations on information security matters, including representing the organisation in cross-community issues.
- Ensuring that contingency plans and disaster recovery plans are reviewed and tested on a regular basis.

- Representing the organisation on internal and external bodies that relate to security.
- Ensuring the systems, application and/or development of required policy standards and procedures in accordance with needs, policy and guidance set centrally.
- Approving system security policies for the infrastructure and common services.
- Providing an incident and alert reporting system.
- Providing advice and guidance to Information Governance and users where applicable on:
    - Policy Compliance
    - Incident Investigation
    - Security Awareness
    - Security Training
    - Systems Accreditation
    - Security of External Service Provision

6.5. Caldicott Guardian (Children's Services and Health and Care Services only)

The Caldicott Guardians are responsible for:

- Championing confidentiality issues at SIRO/senior management team level
- Supporting and facilitating information sharing
- The overseeing of disclosures involving patient and client identifiable information
- Ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures.
- The investigation of incidents where actual or alleged breach of confidentiality have occurred. These incidents will be reported to the Information Security Manager and discussed with the SIRO group.

6.6. Data Protection Officer Responsibilities

The Data Protection Officer is responsible for:

- advising the Information Governance and Risk Manager/Information Security Manager on breaches and the recommended actions as they affect their responsibilities;
- advising users of information systems, applications and networks on their responsibilities under the Data Protection Act/GDPR, including Subject Access.
- encouraging, monitoring and checking compliance with the Data Protection Act/GDPR;
- ensuring that appropriate data protection registration is maintained for organisation's systems and information;
- liaising with external organisations on data protection matters;
- promoting awareness and providing guidance and advice on the Data Protection Act/GDPR
- providing advice on handling Subject Access Request.

6.7. Corporate Directors / Line Managers

Corporate Directors and Line Managers are responsible for:

- Ensuring that the security of the organisation's information assets (e.g. information, hardware and software used by staff and, where appropriate, by third parties) is consistent with legal and management requirements and obligations.
- Ensuring that employees, temporary and contracted staff, contractors, elected members and third parties acting for the council conform with System Security Policies and Security Operating Procedures.
- Understanding and reducing risk to information risk within the directorate.
- Assigning ownership to information assets.
- Ensuring that their employees are aware of their security responsibilities.
- Ensuring that their employees have undergone suitable security training.
- Assigning system owners for any information systems.

- Ensuring directorate arrangements are in place to manage information risk.
- Provide assurance that information assets are protected against security risks and threats.

6.8. All Users

All council employees, temporary and contracted staff, contractors, elected members and third parties acting for the council have a statutory duty of confidentiality to protect information and only use it for the purposes for which it was intended.

All users have a duty to:

- Conform to System Security Policies and Security Operating Procedures
- Be aware of their security responsibilities
- Attend suitable security training when arranged
- Safeguard hardware, software and information in their care
- Prevent the introduction of malicious software on the organisation's IT systems
- Report on any suspected or actual breaches in security.
- Be aware that any breach of confidentiality is a serious matter which may result in disciplinary action by the council or the appropriate professional regulatory body.

7. VALIDITY OF POLICY

This policy will be reviewed annually by the Information Security Manager.

Associated information security standards will be subject to an on-going development and review programme.

8. AUDIT DETAILS

Compliance with the policy will be audited according to Information Governance Standards which are subject to routine and statutory assessment and linked internal/external audits.

9. REFERENCES

Related documents include:

- All Policies and Procedures relating to information management and technology security and confidentiality.

- The Data Protection Act 1998 (DPA) which amongst other things requires departments and agencies to process personal data 'fairly' and 'lawfully'.

  Personal data means information about identifiable living individuals and includes both facts and opinions about the individual.

  The DPA does not just apply to data held on computers. Any set of data held are potentially disclosable. This includes any references to an individual in any document, file, folder or e-mail, including e-mails still in the "deleted" folder. Although there has been a tendency to consider e-mails as an informal or ephemeral way of communicating, the data they contain is subject to the same disclosure provisions as data elsewhere. Directories containing names, telephone numbers, e-mail addresses, etc also fall within the scope of the Act.

- The Human Rights Act 1998 incorporated the European Convention on Human Rights into domestic law. Under this Act a UK citizen is be able to assert their Convention rights through the national courts without having to take their case to the European Court of Human Rights.

- The Freedom of Information Act 2000 provides for a general right of access to information held by departments, subject to certain restrictions (e.g. the privacy rights of the individual). The act also amends certain provisions of the Public Records and Data Protection Acts and applies to a wide range of public authorities. The act gives a general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions. Collectively these place a duty on departments and agencies to manage records, including e-mails, in such a way that their provisions can be complied with.

- Obscene Publications Act 1964 - All computer material is subject to this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it. A computer disk, including the principal hard disk of the computer, can constitute an obscene article for the purposes of this Act if it contains or embodies matter that meets the test of obscenity. 'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, offering for sale or for lease. Material posted to a newsgroup, forum or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to include the originator or poster of the item.

- Telecommunications Act 1984 - The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under s.43 of this Act.

- Protection of Children Act 1999; - This Act make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

- Copyright, Design and Patents Act 1988 - Copyright law applies equally to the Internet as it does to paper material. Many web sites contain a copyright notice detailing how the material they contain may be used. If you want to print out a Web page or attachment, or copy-and-paste anything from a Web page or attachment into a document of your own, you should obtain the permission of the copyright owner. For any use beyond everyday web-browsing, permission should be obtained.

- Protection from Harassment Act 1997; Sex Discrimination Act 1975; Race Relations Act 1976 - Harassment and discrimination are unlawful, whether or not the use of work-based communications facilities has played a role.

- Computer Misuse Act 1990 - This Act makes it an offence for an unauthorised person to access knowingly a program or data or for such a person to modify knowingly the contents of a computer.

- Criminal Justice Act 2003 – This act amends the law relating to police powers, bail, disclosure, allocation of criminal offences, prosecution appeals, autrefois acquit, hearsay, propensity evidence, bad character evidence, sentencing and release on licence.