



# Information Security Policy

## Document Version Control

Organisation	Cumberland Council
Document Title	Information Security Policy
Filename	Cumberland Council_Information Security Policy
Document Status	Final
Author	LGR Legal and Democratic Services – Data Assurance Group
Document held by (name/section)	Legal and Democratic Services
Contact	<a href="mailto:security@cumberland.gov.uk">security@cumberland.gov.uk</a>
Date of publication	1 April 2023
Next review date	1 April 2024
Version Number	1.0
Approval date and by who (delegated/ committee)	Delegated – Chief Executive and Senior Information Risk Owner
For internal publication only or external also?	Both
Document stored on Council website or Intranet?	Intranet

## Change History

Version	Date reviewed	Reviewed by	Description of revision
0.1	10/02/2022	Information Security Officer	Draft policy based on existing CCC policy
0.1	10/02/2023	Information Security Manager	Review/approval of changes
0.2	20/03/2023	Senior Information Governance and Data Protection Officer	Applied consistency to Roles and Responsibilities to align with other LGR policies for new authorities

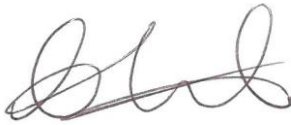

## Document Approval

This document requires approval by the council's Senior Information Risk Owner (SIRO):

Version	Approval Date
1.0	14/04/2023

This Policy will be reviewed by the Information Security Manager on an annual basis from the date of formal approval by the Authorised Signatory (below).

## Authorised Signatory

Officer Name	Position	Version	Signature	Date
Andrew Seekings	Chief Executive	1.0		14/04/2023
Simon Higgins	Director - Resources Senior Information Risk Owner	1.0		14/04/2023

# Contents

Introduction .....	3
Objective .....	3
Scope .....	4
Policy Statement .....	4
Legislation .....	4
Definitions .....	6
Responsibilities .....	7
Validity of Policy .....	10
Audit .....	10
Contacts and Further Information .....	10

## Introduction

This document defines the Information Security Policy for Cumberland 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)

## 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.

## Scope

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

## Policy Statement

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

## 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:

- Data Protection Act 2018
- UK General Data Protection Regulation (UKGDPR)
- 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
- Privacy and Electronic Communications Regulations 2003
- 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.

## Definitions

Article 4(1) UKGDPR/Chapter 2 Data Protection Act 2018 defines ‘**Personal Data**’ as “...*any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as:*

- a name
- an identification number i.e., CCC Employee Number
- location data i.e., home address
- an online identifier

**Special Category Data** (formerly ‘Sensitive Personal Data’) is defined at Article 9(1) UKGDPR as “...*data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation...*”.

Special Category Data also includes information relating to criminal convictions and offences.

The type of data that has been lost or disclosed will also be considered and can generally be seen as falling within the following categories:

### **Public Data**

Data or information intended for public use which can be made public without any negative impact to the Council.

### **Internal Data**

Data or information about the day-to-day business of the Council. This may or may not be shared with third parties subject to contract or a suitable Information Sharing Agreement being in place. This will have some impact on the Council but this is likely to be minor.

### **Confidential or Sensitive Data**

Data or information of a sensitive, personal or restricted nature, including Intellectual Property Rights. The data may only be shared with appropriate people within the Council or those with whom the Council has a suitable contract or Information Sharing Agreement in place. Loss or disclosure of this data or information will have a more serious or even significant impact on the services being delivered to the individual(s) concerned and the Council. It would be likely to be classified as a data breach under the GDPR.

## Highly Confidential Data

Data or information that if released would cause significant damage to the Council and its activities or reputation. This may or may not include personal and sensitive personal data, or data regarding the security of the town or those within it. Loss, disclosure, or unauthorised access would be likely to lead to a data breach under the GDPR. Access to this type of data would be highly restricted and is likely to be available to the necessary persons on a 'need to know' basis only.

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.

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 2018?
- 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:

[dataprotection@cumberland.gov.uk](mailto:dataprotection@cumberland.gov.uk)  
[security@cumberland.gov.uk](mailto:security@cumberland.gov.uk)

## Responsibilities

### Chief Executive

The Chief Executive as Accounting Officer has delegated the overall security responsibility for security, policy and implementation to the Senior Information Risk Owner (SIRO)

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

## **Senior Information Risk Owner (SIRO)**

The Senior Information Risk Owner (SIRO) is responsible for the council's approach to managing information risk, including:

- acting as corporate champion for information governance including security and data protection
- providing a focus for the management of information governance at a senior level
- ensuring that a Data Protection Officer is identified
- ensuring that the council has identified an Information Security Manager
- ensuring that the council has appropriate information security policies in place
- providing advice and reports in respect of information security incidents/risks
- assessing how the council's strategic priorities may be impacted by these incidents/risks and how they can be managed, resourced and scrutinised effectively

To manage identified risks the SIRO is supported by a group of professionals, who can provide advice on the operational and technical aspects of effect data management

The Senior Information Risk Owner is required to be registered with the [NHS Digital - Organisation Data Service](#)

This includes the appointment of one or more Deputy SIROs, usually the Chief Legal and Monitoring Officer or Assistant Director - ICT.

## **Deputy Senior Information Risk Owner(s)**

Authorised either jointly or alone, to act in the absence of the SIRO to:

- make decisions regarding referrals to the ICO,
- chair the weekly SIRO Review Meeting
- consider the risks and activity contained in the SIRO Data Breach Report as supplied by the Data Protection Officer.

## **Chief Legal and Monitoring Officer**

The council's Chief Legal and Monitoring Officer is responsible for providing legal opinion as requested by the Chief Executive or SIRO.

The Information Security Manager is responsible for:

- working alongside the Data Protection Officer to ensure the organisational and technical requirements of the UK General Data Protection Regulation (UKGDPR) are fully implemented
- 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, Data Protection Officer, Caldicott Guardian and other senior staff
- 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 to employees on:
  - compliance
  - incident investigation
  - awareness/training
  - system accreditation
  - external service provision

**Data Protection Officer**

The council is required as a public authority to have a Data Protection Officer (DPO) who is responsible for:

- monitoring data protection compliance
- providing advice, guidance and training to employees and members
- maintaining data protection documentation
- acting as the point of contact for data protection issues with the Information Commissioners Office
- working alongside the Information Security Manager to ensure the organisational and technical requirements of the UK General Data Protection Regulation (UKGDPR) are fully implemented

**Caldicott Guardian**  
(Children’s Services and Adult Social Care Services only)

Supports the SIRO and acts as the conscience of the organisation and is responsible for protecting client and service-user confidentiality.

The Caldicott Guardian is required to be registered with the [NHS Digital - Organisation Data Service](#)

**Executive Directors/Line Managers**

Executive Directors and Line Managers are responsible for:

- ensuring that all employees complete mandatory Information Security and Data Protection eLearning on an annual basis
- 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 directorate arrangements are in place to manage information risk

- provide assurance that information assets are protected against security risks and threats

## Employees

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:

- complete mandatory Information Security and Data Protection eLearning on an annual basis
- conform to System Security Policies and Security Operating Procedures
- be aware of their security responsibilities
- 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.

## Validity of Policy

This policy will be reviewed annually by the Information Security Manager and signed off by the Senior Information Risk Owner/authorised Deputy. Associated information security standards will be subject to an on-going development and review programme.

## Audit

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.

## Contacts and Further Information

Data Protection

Email: [dataprotection@cumberland.gov.uk](mailto:dataprotection@cumberland.gov.uk)

Information Security

Email: [security@cumberland.gov.uk](mailto:security@cumberland.gov.uk)