North Somerset COUNCIL

# Corporate Information Security Policy

## Version 3_1

| | |
|---|---|
| **Author** | Mike Riggall |
| **Date Approved** | 25 May 2022 |
| **Review Date** | 31 May 2023 |

**Contents**

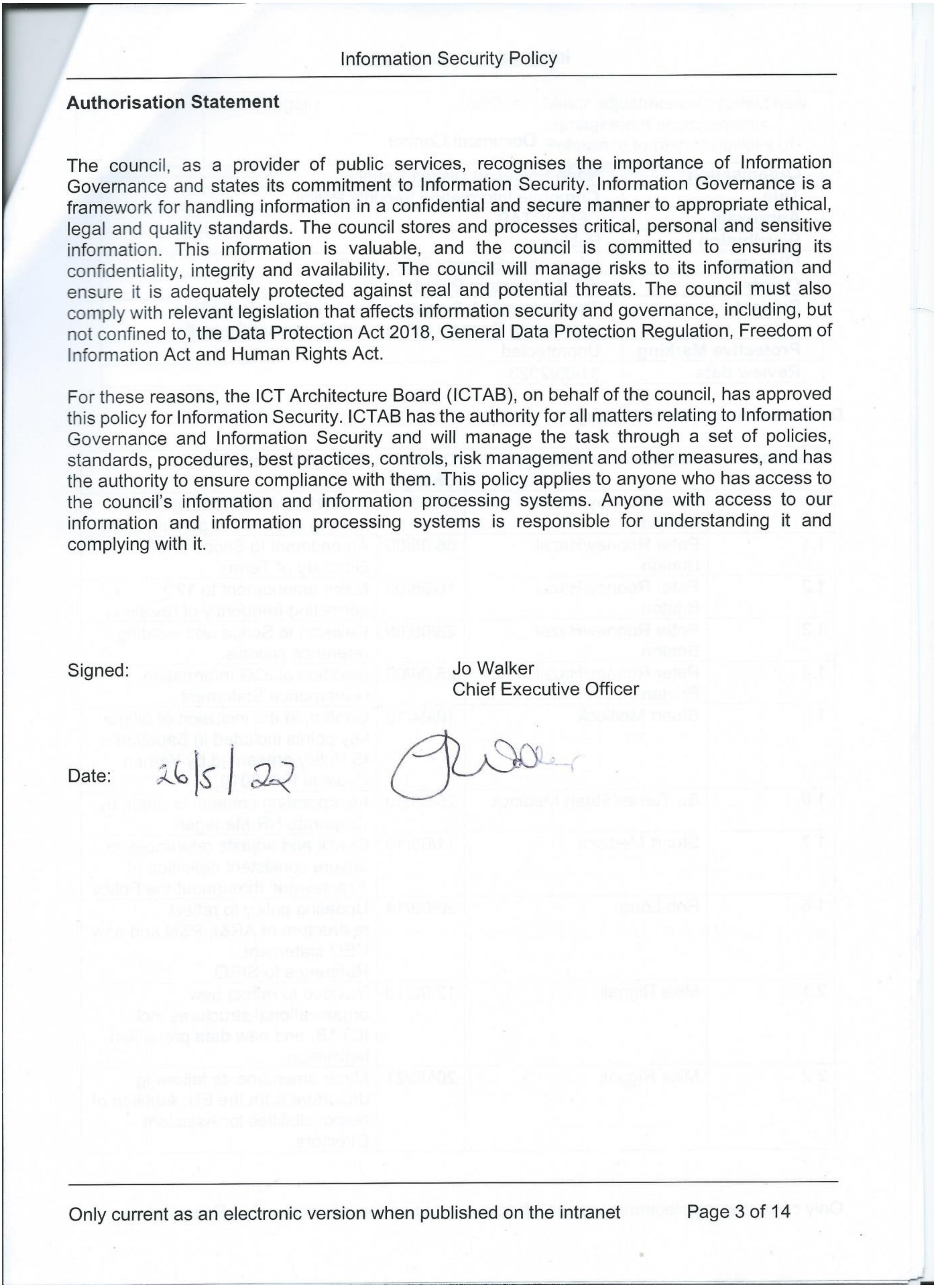
## Authorisation Statement

The council, as a provider of public services, recognises the importance of Information Governance and states its commitment to Information Security. Information Governance is a framework for handling information in a confidential and secure manner to appropriate ethical, legal and quality standards. The council stores and processes critical, personal and sensitive information. This information is valuable, and the council is committed to ensuring its confidentiality, integrity and availability. The council will manage risks to its information and ensure it is adequately protected against real and potential threats. The council must also comply with relevant legislation that affects information security and governance, including, but not confined to, the Data Protection Act 2018, General Data Protection Regulation, Freedom of Information Act and Human Rights Act.

For these reasons, the ICT Architecture Board (ICTAB), on behalf of the council, has approved this policy for Information Security. ICTAB has the authority for all matters relating to Information Governance and Information Security and will manage the task through a set of policies, standards, procedures, best practices, controls, risk management and other measures, and has the authority to ensure compliance with them. This policy applies to anyone who has access to the council’s information and information processing systems. Anyone with access to our information and information processing systems is responsible for understanding it and complying with it.

Signed: Jo Walker
Chief Executive Officer

Date:



## Authorisation Statement

The council, as a provider of public services, recognises the importance of Information Governance and states its commitment to Information Security. Information Governance is a framework for handling information in a confidential and secure manner to appropriate ethical, legal and quality standards. The council stores and processes critical, personal and sensitive information. This information is valuable, and the council is committed to ensuring its confidentiality, integrity and availability. The council will manage risks to its information and ensure it is adequately protected against real and potential threats. The council must also comply with relevant legislation that affects information security and governance, including, but not confined to, the Data Protection Act 2018, General Data Protection Regulation, Freedom of Information Act and Human Rights Act.

For these reasons, the ICT Architecture Board (ICTAB), on behalf of the council, has approved this policy for Information Security. ICTAB has the authority for all matters relating to Information Governance and Information Security and will manage the task through a set of policies, standards, procedures, best practices, controls, risk management and other measures, and has the authority to ensure compliance with them. This policy applies to anyone who has access to the council's information and information processing systems. Anyone with access to our information and information processing systems is responsible for understanding it and complying with it.

Signed: Jo Walker
Chief Executive Officer

Date: 26/5/22

Document Control

| | |
|---|---|
| **Organisation** | North Somerset District Council |
| **Title** | Corporate Information Security Policy |
| **Approvals** | CEO, ICTAB |
| **Distribution** | Public |
| **Filename** | Information Security Policy v2_3 |
| **Owner** | ICT Architecture Board |
| **Subject** | The Corporate Information Security Policy formalises Information Security within North Somerset Council |
| **Protective Marking** | Unprotected |
| **Review date** | 31/05/2023 |

**Document Amendment History**

| **Revision No.** | **Originator of Change** | **Date of Change** | **Change Description** |
|---|---|---|---|
| 1 | Peter Rooney/Hazel Brinton | 26/03/09 | Amendments to wording and making specific the generic areas |
| 1.1 | Peter Rooney/Hazel Brinton | 06/05/09 | Amendment to Scope and Glossary of Terms |
| 1.2 | Peter Rooney/Hazel Brinton | 16/06/09 | Minor amendment to 12.1 correcting frequency of revision |
| 1.3 | Peter Rooney/Hazel Brinton | 23/06/09 | Revision to Scope and wording reference schools. |
| 1.4 | Peter Rooney/Hazel Brinton | 25/06/09 | Insertion of IGG Information Governance Statement |
| 1.5 | Stuart Medlock | 19/04/10 | Confirmed the inclusion of all the key points included in Sapphire’s IS Policy presented by Vernon Poole in Feb 2010. |
| 1.6 | Su Turner/Stuart Medlock | 25/05/10 | Incorporating comments made by Corporate HR Manager |
| 1.7 | Stuart Medlock | 11/06/10 | Check and adjusts references to ensure consistent definition of ‘Framework’ throughout the Policy |
| 1.8 | Rob Long | 26/09/14 | Updating policy to reflect restructure of AR&I, PSN and new CEO statement.<br>Reference to SIRO |
| 2.1 | Mike Riggall | 12/02/19 | Revised to reflect new organisational structures incl. ICTAB, and new data protection legislation. |
| 2.2 | Mike Riggall | 20/05/21 | Minor amendments following departure from the EU. Addition of responsibilities for Assistant Directors |
| 2.3 | Mike Riggall | 26/03/22 | Minor adjustments to reflect new management arrangements. |

| | | | |
|---|---|---|---|
| | | | Reference to responsibilities of Caldicott Guardian.<br>Re-alignment of some sections to improve clarity. |
| 3.1 | Mike Riggall | 25/05/22 | Re-drafted to reflect the requirements of the DSP Toolkit and in response to internal audit recommendations. |

## 1. Introduction

1.1 Information is a major asset that North Somerset Council has a duty and responsibility to protect. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

1.2 The purpose and objective of this Information Security Policy is to set out a framework for ensuring that the council's information assets:

- remain confidential;
- maintain their integrity;
- are available when needed, and
- comply with all information-based legislation, regulations, and other obligations.

1.3 The Information Security Policy covers our data protection principles and outlines our commitment to common law and legislative compliance. It is supported by:

- **Information Standards:** standards that apply to all users of the Council's information, and that are designed to meet the control objectives defined within the international information security standard, ISO 27001. Other applicable standards include Public Services Network (PSN) Code of Connection, Payment Card Industry Data Security Standards (PCI DSS), 10 Steps to Cyber Security, the NCSC Cloud Security Principles and the Department for Health DSP Toolkit.
- **Sub-policies:** twelve documents that provide more detail on how the Council will achieve compliance with the Information Standards. One of these, the Personal IS Policy, takes the form of an Acceptable Use Policy that covers user facing technologies such as: email, Internet, remote access and removable media.
- **Baselines:** that define the minimum level of acceptable security.
- **Procedures***:* that provide specific details of how the policy, standards and guidelines will be implemented and how the principles of data protection by design and by default are implemented across the authority.
- **Guidelines:** guidance on aspects of information security that relates to different groups of users.

Together these documents form the council's Information Security Policy Framework.

## 2. Scope

2.1 This Information Security Policy outlines the framework for management of Information Security within North Somerset Council.

2.2 The Information Security Policy, Standards, associated Sub-policies, and Baselines (the Information Security Policy Framework) apply to all Users of the council's ICT or Information, for whatever purpose it is being used, and includes all staff, including temporary staff, contractors and agency workers.

2.3 This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

2.4 Locally-managed schools sit outside the scope of the Information Security Policy, except where Users based in schools are connected to the council's networks or are using the council's IT systems other than those such as the web site which are specifically designed for public access. Council information that is held on schools' equipment is covered, and any schools holding council information will be subject to the Third Party Use of Council's Resource Policy (U04).

2.5 Schools processing their own information and operating their own equipment are not subject to this Policy.

2.6 Schools that continue to fall under the management of the local authority, i.e. non-academies, are required to have and operate their own policies for information security and governance. In the event of an information security incident (see Information Security Incident Policy U07), the council will reference compliance with these policies. In the event of a major security incident, the council's Monitoring Officer may withdraw the delegation of policy in this area to the school.

## 3. Risks to North Somerset Council

3.1 When information and other IT systems are unavailable, the ability of the council to deliver its services is significantly diminished.

3.2 Data and information collected, analysed, stored, communicated and reported may be subject to theft, misuse, loss and corruption.

3.3 Information processed by the council may not be available due denial of service or other malicious activity originating outside or within the organisation.

3.4 Poor education and training, misuse and breach of security controls of information systems may result in data and information being put at risk, may be used to misrepresent the council and result in the ineffective use of the council's resources.

3.5 Information security incidents can give rise to embarrassment, financial loss, non-compliance with standards and legislation as well as possible judgements and fines against the council.

## 4. Statement of Management intent

4.1 It is the policy of the council to ensure that information will be protected from a loss of:

- Confidentiality: so that information is accessible only to authorised individuals.
- Integrity: in order to safeguard the accuracy and completeness of information and processing methods.
- Availability: so that authorised Users have access to relevant information when required.

4.2 We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);
- Accurate and kept up to date;
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (‘storage limitation’);
- Processed in a manner that ensures appropriate security of the personal data.

4.3 We uphold the personal data rights outlined in the GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

4.4 We will follow the principles of the ISO27000 series, the International Standards for Information Security, to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation in all matters relating to information security and data protection.

4.5 We will comply with all assurance and accreditation schemes which are appropriate for us a local authority, including:

- Public Services Network (PSN) Code of Connection
- Data Security and Protection toolkit (DSPT)
- Cyber Essentials Plus
- Payment Card Industry Data Security Standards(PCIDSS)

4.6 In line with legislation, we will appoint a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

## 5 Principles

5.1 Regulatory, legislative and contractual requirements relating to matters of information security and data protection will be incorporated into the Information Security Policy, Standards, and associated Sub-policies outlined previously in paragraph 1.3.

5.2 The requirements of the Information Security Policy, Standards, and associated Sub-policies will be incorporated into the council's operational procedures and contractual arrangements.

5.3 The Corporate Leadership Team (CLT) has appointed the ICT Architecture Board (ICTAB) as the governance board overseeing all aspects of information security and data protection including a responsibility to review and make recommendations on information security policy, policy standards, directives, procedures, incident management and security awareness education on behalf of CLT.

5.5 Information security education and training will be available to all Users and all Users will be required to complete mandatory elements at least once every two years.

5.6 We will establish and maintain policies for the controlled and appropriate sharing of customer and service user and workforce information with other agencies, taking account all relevant legislation.

5.7 Where we rely on consent as the lawful basis for processing personal data, we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. We will ensure that a data subject can withdraw consent at any time through processes which have been explained to them. We ensure that it is as easy to withdraw as to give consent.

5.8 We will undertake annual audits of our compliance as required to comply with legal requirements.

## 6. Responsibilities

6.1 Corporate Leadership Team (CLT) is accountable for:

- approving a framework for managing and overseeing its duties in relation to Information Security as set out in this policy, and
- providing commitment to, and support for, Information Security.

The ICT Architecture Board supports CLT in its role as the governing board for all operational matters relating to information governance and information security.

6.2 The ICT Architecture Board is responsible for:

- being the designated council owner of the Information Security Policy;
- the maintenance and review of the Information Security Policy, Standards, and associated Sub-policies of the Framework;
- the provision of training and education on information security for all Users, and

- other specific responsibilities defined in the associated policies and in its Terms of Reference.

6.3 Directors are accountable for:

- effective procedures which comply with this policy Framework;
- ensuring the procedures used by officers under their line management are managed in accordance with this policy and ensuring that all officers are aware of, and can adhere to, the Information Security Policy;
- support for Information Security in terms of resources and commitment;
- having in place control systems and measures, such as, for example, procedures to ensure the proper care and custody of information used under their line management, and
- ensuring that the Information Security Policy is reflected in job descriptions and roles where appropriate.

6.4 Assistant Directors are responsible for:

- Ensuring that staff processing personal data complete their mandatory Information Governance training at a period not exceeding once every two years;
- Investigating information security incidents and authorising any decision to report to the regulator.

6.5 Managers are responsible for:

- ensuring that all permanent and temporary staff, contractors, partners, suppliers and customers of the council who have access to the Information Systems or information used for council purposes are made aware of and comply with the Information Security Policy, Standards, Baselines and associated Policies.

6.6 The Data Protection Officer is a formal role required as part of the General Data Protection Regulation and who provides advice and guidance to the organisation on all aspects of data protection and information governance. On a day to day basis the transactional aspects of the DPO role is carried out by the Information Governance Team.

6.7 The Caldicott Guardian is a statutory role appointed by CLT the purpose of which is to protect the confidentiality of people’s health and care information and to make sure it is used properly.

6.8 The council’s Information Governance Team function is responsible for:

- reviewing the adequacy of the controls that are implemented to protect the council’s information and recommend improvements where deficiencies are found

- investigate incidents involving failures in the confidentiality, integrity of availability of information and information systems.

6.9 Every User accessing council information is required to adhere to the Information Security Policy, Standards, associated Sub-policies, and Baselines.

6.10 Failure to comply with the Information Security Policy, Standards, associated Sub-policies, and Baselines will lead to disciplinary or remedial action.

6.11 Any breach of this policy is strictly prohibited. ICTAB may suspend access to ICT or information to any User if, in its opinion, there has been or may be, a breach of this policy, or if any use of ICT is considered unacceptable.

6.12 In regard to the scope of this policy, any conduct and or actions which are unlawful or illegal may constitute a personal liability.

6.13 The council's Disciplinary Policy will apply to all employees and temporary employees (not including agency workers), and disciplinary action including dismissal may be taken, in the event of a breach of this policy. The council's disciplinary procedure is available through The Source, or else by application to the Corporate Human Resources Section.

6.14 Elected members may be disciplined through the Standards Committee for Elected Members, on the advice of the council's Monitoring Officer. Elected Members may apply to the Assistant Director Legal and Governance and Monitoring Officer for access to the appropriate procedure.

6.15 Those members of schools' staff to whom this policy applies (see above), will be subject to their own schools' disciplinary procedures and should apply to the relevant Head Teacher for access to them. Disciplinary procedures may be invoked by the council following withdrawal of delegation of this procedure to the school, if in the view of the Council's Monitoring Officer this action is warranted by nature of the seriousness of the breach or likely breach.

## 7. Data Protection by Design and Default

7.1 We shall implement appropriate organisational and technical measures to uphold the principles outlined in section 5. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

7.2 We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

7.3 Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using corporate checklist and DPIA template.

7.4 All new systems used for data processing will have data protection built in from the beginning of the system change.

7.5 All internet-facing information systems regardless of where they are hosted, must be subjected to a detailed penetration test from a CHECK-registered company and the ensuing vulnerability report must be made available to the Information Security Manager. All vulnerabilities identified must be accepted, mitigated or eliminated to the written satisfaction of the ICT Security Manager before any live data is processed within such a system.

7.5 All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

7.6 We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

7.7 In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

7.8 Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

## 6. Commercial Activity

6.1 Users are not permitted to exploit, for personal use or commercial gain, any programs, results, written output or other material developed using council ICT resources, unless such exploitation has been specifically authorised by a Director. The council retains the IPR of all electronic information created using ICT resources.

6.2 ICT resources provided by the council may not be used for commercial activity, for advertising or for fundraising, except for council-related activities, unless such activities have been specifically approved by the chair of ICTAB, Chief Executive Officer or a Director.

6.3 Entering into any personal transaction that involves the council in any way (arranging for delivery of personal goods to a council address, for example) is prohibited.

## 7. Review

7.1 The security requirements for the council will be reviewed by ICTAB and formal requests for changes will be raised for incorporation into the Information Security Policy, Standards, Sub-policies, Baselines, and Procedures.

7.2 This policy, standards and the associated sub-policies will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

7.3 Requests for amendments, clarifications or additions should be made to the Responsible Officer who will make representations to ICTAB as the Accountable body.

## 8. Communication

8.1 The Information Security Policy, Standards, Sub-policies, Baselines and Procedures will be communicated to each User who accesses information and information processing facilities.

## 9. Policy Standards

9.1 The policy standards referred to here are defined in more detail in the "Information Security Standards" document.

## 10. External Advice

10.1 Specialist external advice will be drawn upon where necessary so as to maintain the Information Security Policy, Standards, Sub-policies, Baselines, and Procedures to address new and emerging threats and standards.

## 11. Asset Management

11.1 All relevant assets as defined by ICTAB (and which currently include data, information, software, computers and mobile devices) are accounted for and have an owner. The owner shall be responsible for the maintenance and protection of the asset/s concerned.

## 12 Human Resources Security

12.1 Employee, contractor and third-party terms and conditions of employment/working and any supporting documents, e.g. role profiles, must set out security responsibilities and show adequate screening and declaration processes in place.

## 13 Physical and Environmental Security

13.1 Physical security and environmental conditions must be commensurate with the risks to the area concerned. In particular, critical or sensitive information processing facilities must be located in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls.

## 14 Communications and Operations Management

14.1 Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities must be established.

14.2 The Records Management Policy and associated Retention and Disposal Schedule must be implemented for all information holding systems, both manual and electronic.

## 15 Access Control

15.1 Access to information and information systems must be driven by business requirements. Access shall be granted to, or arrangements made for, Users according to their role, only to a level that will allow them to carry out their duties.

15.2 A formal User registration and de-registration procedure is required for access to all information systems and services.

## 16 Information Systems Acquisition, Development and Maintenance

16.1 Information security risks must be identified at the earliest stage in the development of business requirements for new information systems or enhancements to existing information systems.

16.2 Controls to mitigate the risks must be identified and implemented where appropriate.

## 17 Information Security Incident Management

17.1 ICTAB will define categories of Information Security Incidents which will include a definition of breach.

17.2 All breaches of information security, actual or suspected, must be reported and will be investigated, as detailed in the Information Security Incident Policy (U07). Mitigating action must be taken in a consistent, timely manner and in accordance with the requirements of the UK GDPR.

## 18 Business Continuity Management

18.1 Arrangements must be in place to protect critical business processes from the effects of failure or disasters and to ensure the timely resumption of business information systems.

18.2 Business continuity plans will be produced, maintained and tested, as detailed in the Business Continuity Policy (U09) and the council's overall Business Continuity Plan, which sits outside of the framework.

## 19 Compliance

19.1 The design, operation, use and management of information systems must take into consideration all statutory, regulatory and contractual security requirements.

## 20. Policy Compliance

20.1 If any User is found to have breached this policy, they may be subject to action under the council's Disciplinary Policy. 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, please seek advice from the Information Governance Team.

## 21. Policy Governance

The following table identifies who within the council is Accountable, Responsible, Informed and Consulted with regards to this and the sub-policies with the Information Security Framework. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

| | |
|---|---|
| **Responsible** | Information Security Officer |
| **Accountable** | ICT Architecture Board and SIRO (chair of ICTAB) |
| **Consulted** | Data Protection Officer, Caldicott Guardian, Corporate HR, Information Governance Team, Agilisys |
| **Informed** | All Users of the council’s information and IT systems |

## Appendix A: Glossary

| **Term** | Description |
|---|---|
| **Council** | North Somerset District Council |
| **Baselines** | Establishes the implementation methods for security mechanisms and products. |
| **Data** | A specific fact or characteristic |
| **DPO** | Data Protection Officer – currently the Assistant Director Legal & Governance and Monitoring. |
| **Framework** | The Information Security Policy, the Statement and all associated sub-policies, standards, guidelines and procedures. |
| **Guidelines** | General statements designed to achieve the objectives of the policy by providing a framework within which to implement controls |
| **ICT** | Information Communications Technology. Throughout this policy ICT is defined as hardware, software, information, services and associated devices in the broadest sense used for information processing and communications. ICT includes, *inter alia*, any computer or communications related equipment, PCs, mobile devices, servers, hubs, switches, wireless access points, telephones, printers and all other peripherals. ICT includes the Council's data and voice communications networks of equipment, software and protocols, both Local and Wide Area in definition and extent. And ICT also includes databases, e-mail and any other electronically generated data. |
| **ICTAB** | The ICT Architecture Board is the governing group tasked by Corporate Management Team to ensure the council manages its information systems in accordance with good information security practice. |
| **ISO** | International Standards Organisation |
| **Information** | Information takes many forms and includes:<br>• Hard copy data printed or written on paper<br>• data stored electronically<br>• communications sent by post / courier or using electronic means<br>• stored tape, microfiche or video<br>• speech<br>Information as it is used here means data, information and records as these are traditionally defined in for example, records management literature. They are meant fully inclusively, nothing is excluded which might reasonably be considered information, data or records. |
| **NCSC** | National Cyber Security Centre |
| **Organisation** | The Council |
| **Procedures** | Step by step instructions detailing how policy and standards will be implemented in an operating environment |
| **SIRO** | Senior Information Risk Owner (SIRO) – Assistant Director Legal & Governance and Monitoring, DPO, and chair of ICTAB.<br>Council's lead and champion on information risk and advises CLT on the effectiveness of information risk management across the Organisation. |
| **Standards** | Mandatory activities, actions, rules or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective. The standards are derived from the international security standard ISO 27001 |
| **User/s** | Elected members, management, permanent and temporary staff, contractors, partners, suppliers and customers |