NORTH SOMERSET COUNCIL

Corporate Information Security Policy

Version 1_8

FINAL

Author	
Date Approved	
Review Date	

Contents

Authorisation Statement 3
Document Amendment History 4
1. Introduction 5
2. Scope 5
3. Risks to North Somerset Council 6
4. Statement of Management intent 6
5. Responsibilities 7
6. Commercial Activity 8
7. Review 8
8. Communication 8
9. Policy Standards 9
10. Policy Compliance 10
11. Policy Governance 10
12. Review and Revision 11
Appendix A: Glossary 12

Authorisation Statement

North Somerset Council

Information Governance Statement

The council, as a provider of public services, recognises the importance of Information Governance and 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 central to its work 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, Freedom of Information Act and Human Rights Act.

For these reasons, the Information Governance Group on behalf of the council has approved this policy for Information Security The Information Governance Group has the authority for Information Governance and Information Security and will manage them through a set of policies, standards, procedures, best practices, controls, risk management and other measures, and will have the authority to ensure compliance with them. This policy applies to anyone who has access to the council's information and information processing systems. All such persons are responsible for understanding it and complying with it.

Signed: M. Sanderson Chief Executive Officer

Date: 26/1/15

Document Control

Organisation	North Somerset District Council
Title	Corporate Information Security Policy
Creator	Devon Information Security Partnership (DISP)
Source	DISP, West Midlands LGA, North Somerset Council AUP
Approvals	
Distribution	
Filename	Information Security Policy v1.7
Owner	Information Governance Group
Subject	The Corporate Information Security Policy formalises Information Security within North Somerset Council
Protective Marking	Public
Review date	Annually

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. Reference to SIRO

1. Introduction

1.1 Information is a major asset that North Somerset Council has a duty and responsibility to protect.

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; and are available when needed, and to ensure compliance with all information based legislation, regulations, and other obligations.

1.3 The Information Security Policy is a high level document, and 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; Public Services Network (PSN) Code of Connection; Payment Card Industry Data Security Standards, and mandatory elements of the Government's own Security Policy Framework.
- **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 memory sticks.
- **Baselines:** that define the minimum level of acceptable security.
- **Procedures***:* that provide specific details of how the policy, standards and guidelines will be implemented in particular operational environments.
- **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) applies to all Users of the council's ICT or Information, for whatever purpose it is being used.

2.3 Locally-managed-schools are 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 ICT. Council information held on schools' equipment or files is covered, and any schools holding council information will be subject to the Third Party Use of Council's Resource Policy (U04).

Schools processing their own information and operating their own equipment are not subject to this Policy. Schools 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 Data and information collected, analysed, stored, communicated and reported may be subject to theft, misuse, loss and corruption.

3.2 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.

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

4. Statement of Management intent

4.1 It is the policy of the council to ensure that:

4.1.1 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.

4.1.2 The council has appointed an Information Governance Group (IGG) to review and make recommendations on security policy, policy standards, directives, procedures, Incident management and security awareness education.

4.1.3 Regulatory, legislative and contractual requirements will be incorporated into the Information Security Policy, Standards, and associated Sub-policies.

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

4.1.5 The council will work towards the ISO27000 series, the International Standards for Information Security.

4.1.6 The IGG will define Information Security Incidents, including a definition of breach.

4.1.7 All breaches of information security, actual or suspected, must be reported and will be investigated, as detailed in the Information Security Incident Policy (U07).

4.1.8 Business continuity plans will be produced, maintained and tested, as detailed in the Business Continuity Policy (U09) and the council's Business Continuity policy which is outside of the framework.

4.1.9 Information security education and training will be available to all Users.

4.1.10 Information stored by the council is appropriate to the business requirements and will be processed in accordance with the principles of the Data Protection Act 1998.

5. Responsibilities

5.1 The Executive is accountable for:

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

The Executive has delegated its responsibilities in respect of this policy to the Information Governance Group.

5.2 The Information Governance Group (IGG) 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.

5.3 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.
- ensuring that Information Security policy is reflected in Job Descriptions and roles where appropriate.

5.4 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.

5.5 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.

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

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

5.8 Any breach of this policy is strictly prohibited. The IGG 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 any use of ICT considered unacceptable.

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

5.10 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 on its intranet, or else by application to the Corporate Human Resources Section.

5.11 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 Head of Legal and Democratic Services for access to the appropriate procedure.

5.12 Schools staff (to whom this policy applies, see above) will be subject to their own school's disciplinary procedures and should apply to the Head Teacher for access to them. Disciplinary procedures may be invoked by the council ("LEA") 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.

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 copyright 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 Strategic ICT Client Manager, Chief Executive 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 the IGG and formal requests for changes will be raised for incorporation into the Information Security Policy, Standards, Sub-policies, Baselines, and Procedures.

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.

9.1 Organisation of Information Security

9.1.1 The security of information will be managed within an approved framework through assigning roles and co-ordinating implementation of this security policy across the council and in its dealings with third parties.

9.1.2 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.

9.2 Asset Management

9.2.1 All assets (data, information, software, computer and communications equipment, service utilities and people) are accounted for and have an owner. The owner shall be responsible for the maintenance and protection of the asset/s concerned.

9.3 Human Resources Security

9.3.1 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.

9.4 Physical and Environmental Security

9.4.1 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 housed in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls.

9.5 Communications and Operations Management

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

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

9.6 Access Control

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

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

9.7 Information Systems Acquisition, Development and Maintenance

9.7.1 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.

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

9.8 Information Security Incident Management

9.8.1 Information security incidents and weaknesses must be recorded and mitigating action taken in a consistent and timely manner.

9.9 Business Continuity Management

9.9.1 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.

9.10 Compliance

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

10. Policy Compliance

10.1 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.

11. 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 and council 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	Information Governance Group and SIRO
Consulted	Corporate HR, Unison, Client Team
Informed	All Users of the council's information and IT systems

12. Review and Revision

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

12.2 Policy review will be undertaken by the Responsible Officer. Requests for amendments, clarifications or additions should be made to the Responsible Officer who will make representations to the Accountable body.

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
Devon Information Security Partnership	Representatives of the Local Authorities and other Governmental organisations in the County of Devon. This group initiates and supports good information security practice.
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.
ISO	International Standards Organisation
Information	Information takes many forms and includes: • Hard copy data printed or written on paper • data stored electronically • communications sent by post / courier or using electronic means • stored tape, microfiche or video • speech 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.
IGG	Information Governance Group is the Council's Monitoring Officer, Caldicott Guardian, the Executive Member Finance, Property & Human Resources, the Head of Audit and Assurance and representatives from each Directorate that monitor the implementation of this policy and recommend how the policy should apply to Council activities
Procedures	Step by step instructions detailing how policy and standards will be implemented in an operating environment
SIRO	Senior Information Risk Owner (SIRO) – Head of Legal and Democratic Services. Council's lead and champion on information risk and advises CMT 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