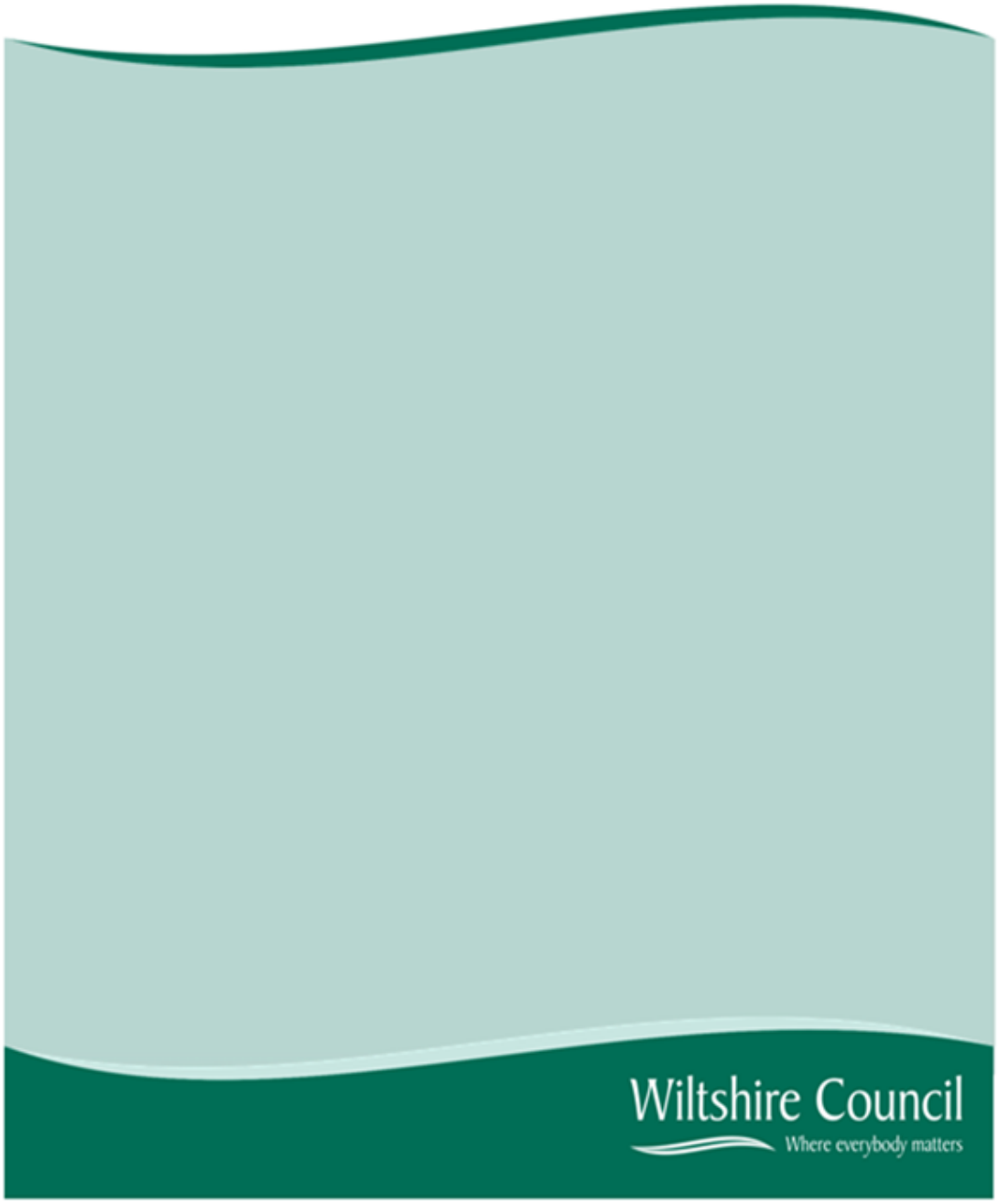
Network Security Policy



Document Control

Reference Number	**Version** 2.0	**Status** Published	**Sponsor(s)/Author(s)** Tim Way, Sarah Davis-Solan
Amendments			
Document objectives: To establish responsibilities for the management of information security risks to the council's networks and to specify principles for their secure and acceptable use			
Intended Recipients: Wiltshire Council Officers			
Group/Persons Consulted: None			
Monitoring Arrangements and Indicators: None			
Training/Resource Implications:			
Ratifying Body and Date Ratified	Information Governance Programme Board September 2017		
Date of Issue	September 2017		
Review Date	September 2018		
Contact for Review	Information Governance		
SIRO signature			

Associated Documentation

Policies

Wiltshire Council controlled documents

- Information security Policy
- Information Governance Policy
- Information Governance Management Framework
- Mobile Working Policy
- Information Asset Change Policy
- Information Incident Management Policy
- Records Management Policy
- Information Classification Scheme

Legal framework

- Computer Misuse Act 1990
- Copyright Design and Patents Act 1988
- Data Protection Act 1998
- Freedom of Information Act 2000
- Health and Safety at Work Act 1974
- Regulation of Investigatory Powers Act 2000

Codes of Practice and Guidance

- British Standards relating to Information Security
- ISO 27000:2013 document series relating to information security.
- IG Toolkit https://www.igt.hscic.gov.uk
- Cyber Essentials. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
- PSN Code of Connection (CoCo) https://www.gov.uk/guidance/apply-for-a-public-services-network-psn-connection-compliance-certificate
- Government End User Device Security and Configuration Guidance https://www.gov.uk/government/collections/end-user-devices-security-guidance

Contents

1. Introduction

This document defines the Network Security Policy for Wiltshire Council (the council) and enables access to, and ensures the security of, council network/s.

It establishes the responsibilities of the council in managing the network and users' responsibilities in using it. It also provides information on taking action to foresee, detect, prevent or rectify security risks which threaten the activities of the council, its partners and its staff.

This policy states clearly: ICT responsibility, the use of the council networks and devices connected to that infrastructure and all users' responsibilities in using such devices.

This policy defines the appropriate use of the council networks and makes users aware of what the council deems as acceptable and unacceptable use of its networks.

2. Scope

This policy applies to:

- All employees of the council, elected representatives, other workers who may not be directly employed by the council (e.g. agency workers, contractors, self-employed consultants, authorised 3rd party suppliers and duly authorised visitors);
- All the council networks, including the telephony network and the data communications network;
- All devices connected to the council networks, including, but not limited to, user devices, printers, servers and network devices;
- External network connections, such as VPN connections;
- Access to internet systems and services.

This policy also covers:

Unauthorised connection of devices to the council networks.

The detection of, and protection and action against threats and data leakage that may cause reputational, commercial or financial harm to the council, its service users and its partners. This includes but is not restricted to the following:

- Viruses
- Denial of Service attacks;
- Hacking internally or from external sources;

- Downloads and uploads of unacceptable material as defined by the Internet & Email Acceptable Use Policy;
- Unacceptable content of outgoing email;
- Filtering of incoming email;
- Unsolicited bulk email;
- Theft, corruption or loss of data or software from external sources;
- Theft of bandwidth.

3. Policy Statement

The council will take necessary action to safeguard the security of the network and contain potential risks to the council, its staff and partners from the consequences of network-related security violations and misuse.

4. Security/Reliability

The council will maintain the security of its networks and information assets in accordance with legislation and Business Impact Assessments (completed by Information Asset Owners) by:

- Ensuring the availability of the network for authorised users;
- Safeguarding confidentiality by implementing controls to protect information flows;
- Preserving integrity by protecting the network from unauthorised or accidental modification.

The council will ensure the network is able to withstand or recover from threats to its availability, integrity and confidentiality. To satisfy this, the council will:

- Protect all hardware, software and information assets under its control. This will be achieved by implementing a secure network architecture with measures such as: firewalls; gateway and device level anti-virus; encryption tools; tested secure configurations and security operating procedures;
- Implement the Network Security Policy in a consistent, timely and cost effective manner.

The council will initiate security audits and self-assessment to ensure compliance with this policy.

All potential and actual security breaches will be investigated and, where appropriate, be reported in accordance with the requirements of the council's incident reporting procedures.

The council will ensure that the latest level of anti-virus software and security patches are installed on all equipment that accesses the network.

The management of remote network equipment should only be conducted by authorised ICT service staff. All network equipment should have a unique and non-default, username and password set to access the device. Only predetermined clients will be configured to access network equipment remotely.

The confidentiality and integrity of data passing over public networks should be maintained in line with the Information Classification Policy, using current industry standard security protocols and encryption.

To meet the requirements of this and other ICT policies, the council will monitor and manage traffic entering and leaving its network. All monitoring will comply with current legislation.

The council is responsible for investigating, containing and resolving breaches of security, and may disconnect, block traffic to/from, impound, or log information about any device using the data network.

The council will perform monitoring and reviews to ensure the networks are performing to the best ability and that no issues are present in the networks.

The council will identify cyber security incidents through monitoring network traffic and system logs for unauthorised access attempts, unauthorised system changes and unusual system responses.

The council will use technical segregation measures between networks and systems with different levels of trust and information sensitivity e.g. between internet facing servers and the internal network, and between test and production systems.

The council's data and telephony networks may only be used for purposes that are in accordance with the aims and policies of the council and for no other reason.

The installation and use of unauthorised software is prohibited and may result in disciplinary action. Applications to use non-standard software on the council equipment must be submitted to the ICT Service Desk as a change request for approval.

Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

Door lock codes will be changed periodically, and following a compromise of the code or a suspected compromise.

Critical or sensitive network equipment will be protected from power supply failures.

Critical or sensitive network equipment will be protected by intruder alarms and fire suppression systems, where appropriate.

Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

All visitors to secure network areas must be authorised by the appropriate council Operations & Transition Manager.

All visitors to secure network areas must be made aware of network security requirements.

All visitors to secure network areas must be logged in and out in accordance with the council procedures for visitors. The log will contain name, organisation, purpose of visit, date, and time in and out.

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The Head of ICT will maintain and periodically review a list of those with unsupervised access.

5. Risk Assessment

The council will carry out security risk assessment(s) in relation to all the business processes covered by this policy.

Risk assessments will cover all aspects of the network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect the network against possible breaches in confidentiality, integrity and availability.

Formal risk assessments will be conducted in line with the council's Risk Management strategy.

6. Documentation

The council will maintain clear, well documented network designs and standard operating procedures covering the correct and secure operation of the network and its components.

The council will ensure that all configuration changes to the network are logged via the change request procedure. All such changes must be reviewed by the Change Advisory Board (CAB).

The council will ensure that business continuity plans and disaster recovery plans are produced for the network.

The council will ensure that disruption to the network is kept to a minimum. Procedures are in place to arrange for network 'downtime' to include notification to end users in advance of scheduled maintenance. Change control documentation will be used on network equipment to ensure that only approved work is conducted and that work is logged.

7. End Users/Staff

User Devices may be connected to the network by any member of staff, provided that it is council equipment and it is used in accordance with the aims and policies of the council and for no other purpose.

Only legitimate, registered users (i.e. those granted permission by the council and holding a valid username and password) are permitted to connect to and use the council networks. Access will be via a secure logon procedure designed to minimise the opportunity for unauthorised access.

Users are not allowed to directly connect their own personal equipment to the council networks as this is in breach of this policy.

Visitors may be given permission to connect laptops to the council network to acquire internet access at the discretion of the Operations & Transition Manager. However, 3rd party laptops must meet the requirements of the council's Third Party Security Standards and the guest must agree to use the connection in accordance with the aims and policies of the council and for no other purpose. They should agree to our existing information security, confidentiality and web policies.

Staff should notify their line manager or a member and the ICT Service Desk if they suspect there has been any unauthorised use of the council network.

All network faults must be reported to the ICT Service Desk where they are logged, managed and reviewed.

The council will ensure that all users of the network are provided with the necessary security guidance, awareness and, where appropriate, training, to discharge their security responsibilities.

Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working. The council operates a clear screen policy that means users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked, or a screensaver password activated, if a workstation is left unattended.

Under the council's Disciplinary Policy and Procedure, ICT are authorised to initiate investigations of users who abuse this policy. Such investigations may result in suspension of access without prior notice, pending resolution of the incident and dependent upon the nature of the offence may involve the Police.

8. Approved 3rd Party Suppliers

The council will ensure that maintenance contracts are maintained and periodically reviewed for all network equipment.

Only council ICT approved contractors are permitted to modify the network infrastructure or install new network equipment.

The council or its approved suppliers are responsible for ensuring that backup copies of network configuration data are taken regularly in accordance with their respective backup policies.

9. External Network Connections

Access to the council network from external locations will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access in accordance with the council Mobile Working Policy.

The council will ensure that all connections to external networks and systems conform to the Network Security Policy, PSN Code of Connection and supporting guidance. Refer to the Architectural Design Guidance -3rd Parties Document for further detail.

Suppliers of cloud services and other information asset hosting will be subject to Information Security risk assessments and ongoing oversight.

Any new connections must be requested and approved via the CAB, and must adhere to the Information Asset Change Policy.

The ICT Network Operations Manager must approve all connections to external networks and systems before they commence operation.

Formal agreements for the exchange of data between organisations must be approved in accordance with the council's information governance procedures, including the completion of information security risk assessments and the creation of information sharing protocols and agreements where necessary.

10. Definitions and explanation of terms

Network

A network is collection of network devices which are connected to give users the ability to share information, and access to resources and applications.

Availability

Networks shall be available and secure for all users at the time when required to perform daily activities.

Network Devices

Items of equipment required in the normal operation of networks, such as Servers, Switches, Routers, Wireless Access Points and Firewalls.

User Devices

User devices are generally equipment used by one person to access and process data.

Confidentiality

This involves ensuring that information is only accessible to those authorised to access it, and the prevention of both deliberate and accidental unauthorised access to the council's systems and data sources.

Integrity

This involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorised modification, of either physical assets or electronic data. There must be appropriate contingency, data backup plans, and security event reporting. The council must comply with all relevant data-related legislation in those jurisdictions within which it operates.

11. Duties (roles and responsibilities)

Senior Information Risk Officer (SIRO)

This policy is issued under the authority of the SIRO, who is responsible for implementing an effective framework for the management of network security and enforcing sanctions where necessary to safeguard the council and its members.

Head of ICT Infrastructure

The Head of ICT Infrastructure will maintain and periodically review a list of those with unsupervised access. Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it.

Network Operations Managers

The ICT Network Operations Manager must approve all connections to external networks and systems before they commence operation

Authorise external visitor requests to connect laptops to the council network. Ensuring laptops have current Anti-Virus protection and that the guest agrees to use the connection in accordance with the aims and policies of the council and for no other purpose and in particular they should agree to our existing information security, confidentiality and web policies.

Authorise visitors to secure network areas.

Responsible for managing the risks of any network device connected to the network and ensuring that any necessary security measures to protect the network are implemented including the prevention and detection of misuse.

Monitoring and reporting on the status of network security within the council, and reporting and investigating any potential breaches.

Learning and Development

The Head of Service for Learning and Development is responsible for including this policy on the Corporate Induction Programme.

User Responsibilities / All Staff

The council will ensure that all users of the network are provided with the necessary security guidance, awareness and, where appropriate, training to discharge their security responsibilities.

All users of the network must be made aware of the contents and implications of the Network Security Policy.

Users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.

The council operates a clear screen policy that means that users must ensure that any equipment logged on to the network must be protected if they leave it unattended, even for a short time. Workstations must be locked if a workstation is left unattended for a short time.

All users have a responsibility to safeguard hardware, software and information in their care and prevent the introduction of malicious software to the council's systems.

Irresponsible or improper actions by users may result in disciplinary action.

12. Guidance

Guidance can and should be sought from a range of people through your Line Manager including the:

- Operations & Transition Manager;
- Operations & Transition Team;
- ICT Service Desk;

13. Review Arrangements

This Policy will be reviewed annually unless an earlier date is agreed by the Executive Management Board or the Information Governance Steering Group.

14. Training / Support

The council will provide guidance to all existing and new employees to help them understand their rights and responsibilities under this policy.

15. Process for monitoring effective implementation

Effective implementation of this policy will be monitored by periodic assurance checks, audits and penetration testing by independent, certified organisations.