# Hebden Royd Town Council IT Security Policy

| | |
|---|---|
| Author | Privacy Worx |
| Version | 2 |
| Next Review Date | 26th August 2026 |

## Contents

# Software Management

## 1. Introduction

1.1. This section sets out how the software which runs on our Council's IT systems and services is managed. It includes controls on the installation, maintenance and use of software, with appropriate procedures for upgrades to minimise the risk to information and information systems.

## 2. Scope

2.1. This policy is applicable to all equipment that connects to the Council's fixed and wireless network.

2.2. This policy should be familiar to all staff involved in the specification, installation and maintenance of software.

## 3. Software Security Management

3.1. All software procurement or installation should only be undertaken with the approval of IT Services or the Clerk.

3.2. There must be a nominated individual or business unit responsible for every item of software deployed on the Council's network.

3.3. Software applications are to be managed by suitably trained and qualified staff to oversee their day to day running, and to preserve security and integrity in collaboration with nominated individual application owners.

3.4. All staff managing software applications shall be given relevant training in information security issues.

3.5. The procurement or implementation of new or upgraded software must be carefully planned and managed in conjunction with IT Services or the Clerk. Any development for or by the Council must document the requirements for Information Security.

3.6. Information security risks associated with the procurement or implementation of new, or upgraded, software must use a combination of procedural and technical controls to mitigate any risks.

3.7. All software implemented should be subject to the Council's release management, version control, change approval and management processes.

## 4. Change Control

4.1. For all Council's owned and managed equipment, formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software.

4.2. All changes to operating systems and ancillary software must be properly authorised and must be tested appropriately before changes are moved to the live environment to ensure there is no adverse impact on Council's operations or security.

## 5. Software Development

5.1. Modifications to vendor supplied software shall be avoided as far as possible, and only strictly controlled essential changes shall be permitted, after agreement with the vendor and IT Services or the Clerk, and the development of interfacing software shall only be undertaken in a planned and controlled manner.

5.2. Upgrades or other changes to locally developed software must be assessed to mitigate any potential risk to information security.

## 6. Software Regulation

6.1. The use of illegal software and using software for illegal activities is not permitted and may lead to disciplinary action.

6.2. All software installed on Council's computer systems must have an appropriate licence covering its intended use.

6.3. Use of software which tests or attempts to break Council's system or network security is prohibited unless the Network Services Manager has been notified and has given authorisation.

6.4. Use of software which causes operational problems, causes inconvenience to others, or which makes demands on resources which are excessive or cannot be justified, will be prohibited.

6.5. Software found on Council's IT systems and services which incorporates malware of any type is liable to be automatically or manually removed or deactivated.

6.6. Any system that monitors the activities of other people, including for the purpose of gathering personal information is not permitted unless authorised by the Director of IT Services or the Clerk and the Secretary and Registrar .

## Network Management

### 1. Introduction

1.1. This section will define how the Council's networks are designed and how IT systems, services and devices are connected to them. It includes appropriate technical and procedural controls to reduce risk and meet the requirements of the Data Protection Policy.

### 2. Scope

2.1. To define the Council's policy for designing, controlling and managing the Council's network.

2.2. Enabling the movement of data that supports the Council's business and disabling the movement of data that hinders the Council's business needs over the networks for which the Council is responsible.

### 3. Definitions

3.1. End User Network Device – any network enabled device which is the initial source or ultimate destination in a data network.

3.2. Network Device – a device such as a switch or router through which data passes on its journey to or from an End User Network Device.

3.3. Network Interface – part of a network device or end user network device that enables it to communicate via a network, there may be more than one interface on a device.

3.4. Local Area Network (LAN) – a computer network that spans a relatively small area, such as a building.

3.5. Network Services manager – The person appointed by the Council as the person responsible for the management of the Council's network.

3.6. System Owner – The manager of individual systems or services such as email or websites. Can include classroom PC groups or LAN partitions.

### 4. Management of the Network

4.1. The Council's network shall be managed by suitably authorised and qualified staff appointed by the Director of IT Services or the Clerk to oversee its day to day running and to preserve its security and integrity in collaboration with nominated individual system owners.

4.2. Planned reconfiguration of the network will use formal, auditable change control procedures and appropriate risk management.

4.3. Where there is a risk to the security or quality of service to the network, the Network Services manager is authorised to make emergency changes to restore service.

4.4. The overall control of the IP address scheme is managed by the Network Services manager, although this may be delegated to nominated system owners for limited IP address management.

4.5. Users of the network are advised that network management procedures may include procedures such as:

4.5.1. Probing devices to test security.

4.5.2. Monitoring of network traffic to detect operational issues.

4.5.3. Recording of network traffic to detect possible policy violations.

4.5.4. Validation that data travelling across the network is legitimate and does not have virus content, is not of an offensive nature, and cannot be detrimental to performance or management of any device or end user device on the network.

4.5.5. Monitoring, filtering and blocking of websites and other services where necessary in order to fulfil the Council's statutory and regulatory responsibilities

## 5. Network Architecture

5.1. The network must be designed and configured to deliver performance, reliability and security suitable for the requirements of the Council.

5.2. The network shall be segregated into separate VLANs on the basis of security requirements. These domains can have controls to prevent unauthorised access to the Council's critical business systems, where appropriate.

5.3. LANs in individual buildings or departments should normally be designed and installed by the network management team. In other cases, the Network Services manager reserves the right to check the installation before connecting it to the Council's core network.

5.4. No changes to the network infrastructure, such as the introduction of a router, switch or wireless access point, is permitted without prior approval from the Network Services manager.

5.5. Records of all active and inactive network device locations and configurations shall be maintained.

## 6. Physical Security and Integrity

6.1. Reasonable measures based on a risk assessment, and regulatory compliance must be taken to protect rooms containing servers, active network devices and patching panels from threats such as fire, water, accidental damage, security breaches and theft.

6.2. Physical access to rooms containing servers, active network devices and patching panels shall be restricted to:

6.2.1. A list of authorised staff maintained by the relevant system or Network Services manager.

6.2.2. Other individuals providing that their entry has been approved by the relevant system or Network Services manager.

6.3. Any device that is running a service that conflicts with centrally managed services such as DHCP, etc. must not be connected to the network without prior agreement with the Network Services manager.

### 7. Controlling Access

7.1. Access control procedures must provide adequate safeguards through robust identification and authentication techniques.

7.2. Only devices owned by the Council or recognised partner organisations may be connected to the wired network, except under special circumstances, approved by the Network Services manager.

7.3. Personal devices may be used on the wireless network only after registration and authentication.

7.4. All devices connecting to the Council's network both wired and wireless must conform to Council's policies.

7.5. Remote administrative connection to the Council's network and resources will only be permitted from authorised users and devices over suitably secured connections.

## User Management

### 1. Introduction

1.1. This section governs:

1.1.1. The creation, management and de-provisioning of user accounts.

1.1.2. The granting and revocation of authorised privileges associated with a user-account.

1.1.3. The authentication (usually a secret password) by which the user establishes their right to use the account.

### 2. Scope

2.1. This section applies to all accounts on Council's IT systems and services directly connected to networks which are managed by the Council. This includes operating system (Windows, Linux, Solaris etc.), and application software accounts (HR, Accounts, Database, etc.).

2.2. This document includes statements on:

2.2.1. Access Control

2.2.2. Managing Privileges

2.2.3. Authentication/Password Management

### 3. Access Control

3.1. Manual creation, deletion and changes of user accounts and privileges must be carried out by trained and authorised staff.

3.2. Automated creation of user accounts will be driven by authorised feeder systems including but not restricted to HR according to criteria agreed with the service owners.

3.3. The person enacting any change in a user account must be different from the one authorising/requesting the change.

3.4. Logs will be kept of all account creation/deletion/changes.

3.5. Account details will only be divulged to the user after proof of identity has been established.

## 4. Managing Privileges

4.1. A user account should have the least privilege which is sufficient for the user to perform their role within the Council and access to information and information systems and services must be driven by business requirements.

4.2. Changes in the privilege of an account must be authorised by the user's line manager or a nominated "owner" of the information system to which the account affects.

4.3. Users' privilege rights will be periodically reviewed.

4.4. Procedures shall be established to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, a user changes their role, or a user leaves the Council.

4.5. User accounts should be disabled immediately once the user leaves the Council or after a period agreed with HR. The user's data will not be deleted until after a period agreed with Human Resources, IT Services or the Clerk management and service owners.

4.6. Users should be informed of their responsibility to inform information system owners of any change in their role which might affect their privileges. IT Services or the Clerk should be informed as part of the starters/leavers process.

## 5. Managing Elevated Privileges

5.1. Users whose work requires system administration access will be given a separate specialist account for this purpose, in addition to their standard user account.

5.3. System administration accounts may use the same password policy as other accounts, but on some systems may have a separate password policy, as required by that system/service.

5.4. In all other ways, these system administration accounts should be managed and the user is responsible for them similarly to standard accounts.

## 6. Authentication/Password Management

6.1. All users will have a unique identifier for any Council's IT system and services.

6.2. The user responsible for their account will keep the accounts authentication details secret and will not divulge it to any other person for any reason.

6.3. The account must not be used by the user where there is a possibility that the account details may be revealed.

6.4. Passwords can only be changed by the user or suitably trained and authorised staff.

6.5. If a user suspects their password is no longer secret it must be changed immediately and the system “owner” notified.

## Wireless Communication

### 1. Introduction

1.1. This section sets out how wireless communications equipment and users connect to the Council’s networks. The policy prohibits access to the Council’s internal networks via any unsecured wireless communication mechanisms, other than those explicitly mentioned in the policy. Only wireless systems that meet the requirements of this policy and are approved by IT Services or the Clerk can be connected to the Council’s networks.

### 2. Scope

2.1 This section covers all wireless data communication devices (e.g. personal computers, cellular phones, smartphones, tablets, PDA’s etc.) connected to any of the Council’s internal networks. This includes any form of wireless communication device capable of transmitting data. Wireless devices and/or networks without any connectivity to the Council’s networks do not fall under the purview of this policy.

IT Services or the Clerk must approve exceptions to this policy in advance.

### 3. Wireless Policy Statement

3.1. Statement of Authority

3.1.1. Responsibility for Wireless communication resources resides with IT Services or the Clerk.

3.1.2. IT Services or the Clerk must approve all installations of Wireless access points across all sites. Policies and guidelines for deployment of these systems are essential to prevent interference between different implementations, other uses of the wireless spectrum, and maintain a quality of service connection to a diverse user community.

3.2. Council’s Users Access to Wireless

3.2.1. Wireless access to the Council’s network, is provided by the agreed Council’s supported wireless access service.

3.2.2. All wireless access to the Council’s network will be encrypted and authenticated, using approved protocols and infrastructure.

3.3. Visitor Access to Wireless

3.3.1. Wireless access for visitors to the Council, will be available at all facilities where wireless access has been deployed.

3.3.2. Wireless access for visitors is provided through an encrypted connection with a temporary password provided by reception on request.

3.3.3. Temporary passwords will be pre-set to expire after the minimum period necessary (typically 1 day).

3.3.3. Wireless access for all visitors will be managed through a web-based authentication system.

3.3.4. Wireless access for visitors is restricted to basic web access.

3.4. Operational documentation including coverage locations, end user documentation and service information can be found at: TBA

3.5. Wireless Request Procedure

Requests for wireless networking can be made to IT Services or the Clerk using the Wireless Request Procedure and any request must be made with the approval of the appropriate Manager and must outline how the request supports the business needs and aims of the Council.

### 4. Definitions

• Wireless Network: the network technology that uses radio frequency to connect computing devices to a wired port on the Council's network.

• Wireless infrastructure: The wireless access points, antennas, cabling, power and network hardware associated with the deployment of a wireless network.

• Access Point: A network device that serves as a common connection point for devices in a wireless network. Access points use wireless antennas instead of wired ports for access by multiple users of the wireless network. Access points are shared bandwidth devices, and are usually connected to the wired network.

• Coverage: The physical area where a level of wireless connectivity is available.

## Use of Computers

### 1. Introduction

1.1. This section defines the acceptable actions of any individual who interacts with the Council's IT systems and services. The individual may be an anonymous user of public services (for example, browsing the Council's web pages) or they may be an authenticated user of authorised services (for example sending and receiving Council's email). To be covered by this section, the individual will, either actively or passively, make decisions which in turn cause some computation to be done on Council's IT systems and services.

### 2. Scope

2.1. This section applies to all users of the Council's IT systems and services.

2.2. Unless explicitly stated otherwise in this policy, the Acceptable Use Policy applies to all users of the Council's IT systems and services.

### 3. Faculty or Department Policies and Regulations

3.1. Where necessary a Proper Officer may request to implement different policies relating to the use of Council's IT systems and services for which they have responsibility, subject to agreement with the Head of IT Services or the Clerk.

## 4. Acceptable Use of Council's IT Facilities

4.1. Subject to clauses in section 5 below, the Council's IT systems and services may be used for any lawful activity which furthers the aims of the Council and is consistent with the policies of the Council, both at the time of use and in the reasonably foreseeable future after the time of use.

4.2. Personal use: Subject to clauses in section 5 below, authenticated individuals are allowed to make reasonable use of the Council's IT systems and services provided that the use does not interfere with the performance of their duties, cause financial loss to the Council or cause any difficulty or distress to others.

4.3. Commercial use: A user must obtain explicit permission from the appropriate Manager to use the Council's IT systems and services for commercial gain and this may be subject to a charge

4.4. Authentication (user ids and passwords): where a user has been issued with a user ID and password, the user is presumed to be responsible for all activity attributable to that identity. To that end:

4.4.1. The user will take all reasonable steps to prevent their personal identity from being used by anyone else.

4.4.2. Administrative account holders will also take all reasonable steps to prevent the administrative identity from being used by anyone else. In particular, passwords must be kept unpredictable to anyone except the legitimate account holder.

4.4.3. If a user suspects that their password is no longer secret, they should change their password at the first opportunity.

4.4.4. If you have an impairment that prevents you from entering your own username and password, you are permitted to share these details with your nominated support person.

4.5. Where the user has been allocated a personal computer (such as a laptop or desktop) by the Council, the user should ensure the device is shutdown at the end of the working day.

## 5. Unacceptable Use of Council's IT Systems and Services

The list of unacceptable uses of the Council's IT systems and services listed below is applicable to all Council's IT systems and services and is consistent with the Acceptable Use Policy.

5.1. Any illegal activity.

5.2. The creation, display, download, production, store, circulation or transmission of unlawful material, or material that is indecent, offensive, defamatory, racist, threatening, discriminatory or extremist in any form or medium is strictly forbidden. The Council reserves the right to block or monitor access to such material.

5.3. Staff who requires legitimate access to the types of materials outlined in clause 5.2 must obtain an explicitly signed waiver.

5.4. Continuing to use an item of networking software or hardware after the Head of IT Services or the Clerk has requested that use cease because it is causing disruption to the correct functioning of the Council's systems

5.5. Any attempt to bypass information security safeguards and policies embedded into the Council's network.

5.6. Deliberate unauthorised access to the Council's IT systems and services.

5.7. Using "open access" computing facilities (such as classroom or library computers) for recreational or other non-Council work when there are others waiting to use the resource.

5.8. Authenticated sessions: a user must not leave an authenticated (i.e. logged in) session unattended without first invoking a password protected screensaver or similar device.

5.9. Users must not in any way cause any form of damage to the Council's IT systems and services or the associated hardware.

5.10. Users must comply with any other policies that relate to the use of IT systems and services that the Council may introduce from time to time

## 6. Protecting Against Unknown or Malicious Code

The Council will put in place appropriate measures to protect against the possible risk of unknown or malicious code infecting devices. These protective measures will include:

6.1. Files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

6.2. A combination of proactive measures must be used to help manage the risk of malicious code being run on Council's IT systems and services. A combination of the following measures is recommended:

6.2.1. Deploying antivirus software developed by a reputable supplier, which should be kept fully up to date and used to scan all files: downloaded from the internet, received as attachments to email (or other forms of messaging) and all removable media when inserted.

6.2.2. Advising computer users to avoid running software or opening files obtained from untrusted sources and to be particularly cautious of accessing files attached to unsolicited email and stored on untrusted media.

6.2.3. Managing support of computers such that privilege to install software is restricted to experienced computer support staff.

## 7. Backups

7.1. Any essential information stored on a laptop or on a PC's local disk must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

7.2. Information system managers are responsible for ensuring that backup arrangements published, or agreed with users of the system, are reliably implemented and that users are informed promptly should there be any problems with, or changes to, the backup arrangements.

# Bring Your Own Device

## 1. Introduction

1.1. This section is intended to address the use in the workplace by users of non-Council owned IT devices such as smart phones, tablets and other such devices to access and store Council's information, as well as their own. This is commonly known as 'bring your own device' and referred to in the rest of this policy as BYOD. The use of BYOD devices to process Council's information and data creates issues that need to be addressed, particularly around data security.

1.2. The Council must remain in control of the personal data for which it is responsible, regardless of the ownership of the device used to carry out the processing. As user you are required to keep secure Council's information and data. This applies equally to information held on the Council's IT systems and services and to information held on an employee's own device.

1.3. Users are required to assist and support the Council in carrying out its legal and operational obligations with regards to Council's data and information stored on your device. Users are required to co-operate with officers of the Council when they consider it necessary to access or inspect Council's data stored on your device.

## 2. Scope

2.1. This section applies to all users of Council's IT Systems and Services.

2.2. This section is to ensure that users understand their role and responsibilities when using BYOD and data offsite and accessing Council's IT systems and services from remote locations.

2.3. This section relates to storing and access to Council's information on a BYOD

2.4. Using BYOD devices.

2.5. Using BYOD from Council's premises.

## 3. Using BYOD in relation to Council's Systems and Services Off Premises

3.1. All BYOD devices should be password protected.

3.2. Any mobile device which is not protected by a password/pin and which attempts to access corporate email will be automatically forced to create a password/pin.

3.3. BYOD devices used to access Council's IT systems and services which are at risk of malware infection should run anti-virus software.

3.4. Users should not store or access personal, confidential or commercially sensitive information on or from any device not owned by themselves or the Council

3.5. Any potential breach of the General Data Protection Regulation or loss of commercially sensitive data should be notified to the Council's Governance team and the user's line manager as soon as possible.

3.6. If a domestic wireless solution is used at the user's premises, it must be made secure, utilising the wireless security features and password included with the wireless solution, to ensure no unauthorised access is permitted.

3.7. When using BYOD devices to access Council's IT Systems and Services it is the responsibility of remote users to ensure that all reasonable measures have been taken to secure the remote machine. This includes the use of physical or software firewalls, ensuring the device operating system and all software supported by the publisher and is patched and up to date.

3.8. Some Council's IT Systems and Services have the ability to remotely delete data and in certain circumstances this may be actioned in order to prevent access to the Council's data. Users should be aware that in the event of this happening, this may also impact the user's personal data

3.9. Should the Council introduce/change 'Mobile Device Management' software, users must adopt the new software to continue using Council's services on such devices.

3.10. The Council reserves the right to withdraw support of BYOD.