IT AND SECURITY POLICY

Date Ratified:	10 June 2025
Meeting:	Finance and General Purpose Committee
Next review date:	June 2028 *(3 yearly review)*
Supersedes:	Councillor IT Policy 2022

CONTENTS

1. PURPOSE AND SCOPE

The purpose of this policy is to detail Thornbury Town Council's (the Council) usage guidelines for the information technology systems including email, document access and storage, instant messaging and video conferencing systems. This policy outlines the expectations, responsibilities, and protocols regarding the use of IT equipment and services. It is designed to ensure that all communications are conducted in a manner that is consistent with the Council's standards and legal obligations as well as reducing risk of an IT related security incident.

This policy applies to all individuals who use the Council's IT resources, including computers, networks, software, devices, data, and email accounts.

The Chief Executive shall ensure that this policy complies with relevant legislation and guidelines.

Definition:

Equipment – is hardware and software

Users – Staff and councillors

2. CONNECTING POLICIES

This policy should be read in conjunction with other relevant policies to ensure a comprehensive understanding of the Council's policy and procedures:

- **Data Protection Policy**
- **Freedom of Information (FOI) Policy**
- **Communications Policy**
- **Code of Conduct**
- **Training and Development Policy**

All users are expected to read and comply with these policies as applicable.

3. PROVISION OF IT EQUIPMENT

3.1 Equipment Provided

The Council will supply IT equipment to enable councillors and staff to perform their duties. For councillors this equipment includes but is not limited to:

- One tablet device suitable for accessing Council materials and participating in online meetings.
- One screen protector or protective case to help safeguard the device.
- Optional peripherals such as a keyboard and mouse to facilitate more efficient working.
- Access to Office 365 or similar software required for word processing, spreadsheets, and communication.
- Adaptive software or hardware (as required)

The equipment for staff will be dependent on the role and responsibilities. The required equipment will be identified by Line Managers and referred to the Chief Executive for approval.

All equipment issued remains the property of the Town Council.

The identification of the equipment requirements will be considered as part of new councillors induction. If during the term of councillors, the equipment develops faults this can be reported to Officers for rectifying.

3.2 Replacement Cycle

IT equipment supplied by the Council will generally be replaced every four years, unless otherwise advised by the Council's IT support provider. The replacement cycle may be adjusted depending on the functionality, condition, and technical relevance of the equipment. An earmarked reserve will be created to ensure the required budget to facilitate this arrangement.

3.3 Usage Conditions

The equipment supplied must be used exclusively for Council-related business. It should not be used for personal or commercial purposes. Councillors are responsible for ensuring that the equipment is handled responsibly. IT equipment may be recalled for maintenance, upgrades, or inspections, and users are expected to comply promptly with such requests.

3.4 Insurance

All IT equipment issued by the Council will be covered under the Council's insurance policy. All users must take reasonable care to safeguard the equipment against loss, theft, or damage.

4. SECURITY

To protect the Council's digital infrastructure and data, all users must ensure compliance with the following:

- Anti-virus software must be kept running at all times.
- Do not open attachments or click on links unless the source can be trusted
- Devices must be protected by a secure password. This password must be a minimum of six characters and include a mix of upper-case and lower-case letters, numbers, and special characters. Always use a strong and separate password for your email; that is, a password that is not used for any other accounts.
- Passwords must never be shared and should be changed if suspected to be compromised.
- Devices must be set to automatically lock after a period of inactivity (five minutes or less).
- Home Wi-Fi networks must be encrypted and users are advised to avoid unsecured public networks.
- Only access systems, applications, and data for which they are authorised.
- Never use another individual's account or impersonate other users.
- Report any accidental access to unauthorised data or systems to the Chief Executive immediately.
- Never facilitate access for others who are not authorised.

- It is prohibited to use external data storage, public cloud storage or file sharing services such as USB drives, portable hard drives, Google Drive or Dropbox.
- Microsoft Two-Factor Authentication (2FA) must be enabled and always used for accessing Council email, Office 365, and related Council systems.
- Any lost or stolen device must be reported to the Chief Executive within 24 hours of discovery.
- When a user leaves the Council all IT equipment must be returned to the office within 48 hours.
- Promptly report any suspected or actual data breaches or suspicious activity.
- Obtain written permission before transferring data to non-Council-managed devices.

5. SOFTWARE

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns. The following guidelines must be adhered to:

- Installation of any software on Council devices must be authorised in advance by the Chief Executive or the designated IT provider.
- Software licenses must be valid and in compliance with copyright and intellectual property laws.
- Council-licensed software must not be duplicated or distributed without explicit permission.
- Users who make use of the Bring Your Own Device must ensure that software used for Council business is up-to-date and protected from viruses or malware.
- Any issues related to software functionality, compatibility, or updates should be reported promptly.

Unauthorised installation or use of software may lead to disciplinary action and could also result in legal liability for the Councillor and the Council.

6. MOBILE DEVICE MANAGEMENT (MDM) SYSTEM

To enhance data protection, manage security risks, and maintain oversight of Council-owned devices, the Council may implement a Mobile Device Management (MDM) system. This system allows the secure configuration, monitoring, and management of mobile devices issued to councillors.

Key aspects of MDM usage include:

- Enforcing security settings, such as password policies and encryption.
- Enabling remote wiping of data in case a device is lost, stolen, or compromised.
- Restricting access to certain apps or functions to reduce the risk of malware.
- Providing IT support teams with remote diagnostic capabilities.
- Device location tracking.
- By accepting and using a Council-issued device, councillors agree to have the device enrolled in the Council's MDM system.

7. BRING YOUR OWN DEVICE (BYOD)

7.1 Overview

Some councillors may prefer to use their own devices, such as smartphones, tablets, or laptops, for Council business. This policy permits the use of personal devices, but only under strict conditions that ensure the protection of Council data. The Council reserves the right to revoke BYOD privileges if the conditions of this policy are not followed.

Councillors should note that if personal equipment or email addresses are used for Council-related work, they may be subject to scrutiny in the event of a Freedom of Information (FOI) or data access request received by the Council.

7.2 Requirements

Councillors must ensure that their personal devices meet all the conditions detailed in section 4 – Security as well as the following:

- Personal devices must not be rooted (android) or jailbroken (iOS), as this compromises device security.
- Councillors using their own devices are encouraged to use the web applications and online portals for storing documents and not to download documents to their personal devices.
- Councillors are not permitted to download or store any confidential Council documents locally on their personal devices.
- If a Councillor's term ends, or if there is a data breach or virus infection, all Council-related data must be made available to Officers.
- Personal devices used under BYOD are not subject to the Mobile Device Management System unless explicitly agreed upon.

7.3 Support and Liability

While basic assistance may be provided for connectivity issues, Councillors are primarily responsible for the operation and maintenance of their personal devices. Operating system or hardware-related problems must be resolved with the device manufacturer or service provider. Any expenses associated with the use of personal devices, including data plans or repairs, are the responsibility of the Councillor.

7.4 Insurance

Personal devices used for Council business are not covered under the Council's insurance policy. Councillors who choose to use their own devices are strongly advised to ensure they have adequate insurance coverage in place to protect against loss, theft, or damage.

8. NETWORK, WEBSITE & EMAIL

The Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

The Council has acquired a gov.uk domain, as recommended by guidance, to support good practice and assist in compliance with data protection requirements.

The Council's website must meet **WCAG 2.2 AA** standards.

All staff will be issued a gov.uk email address, while councillors are expected to use their dedicated gov.uk address for Council related communications.

Email accounts provided by the Council are for official communication only. Emails should be professional and respectful in tone and compliant with the Council's Communications Policy. Confidential or sensitive information must not be sent via email unless it is encrypted.

Users should be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

Emails should not be forward to third parties without the original sender's permission.

The Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

9. TRAINING

The Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All training will comply with the Council's Training & Development Policy.

10. BREACH AND ENFORCEMENT

A declaration form, included as Appendix 1, must be signed by all users issued with Council IT equipment.

Any breach of this policy will be treated as a serious matter and may result in disciplinary action, the suspension of IT privileges and further consequences as deemed appropriate. Breaches of this IT policy may also constitute a breach of connecting policies.

APPENDIX 1 - DECLARATION

IT USAGE AND SECURITY POLICY DECLARATION FORM

I acknowledge that I have received, read, and understood the Councillor IT Usage and Security Policy issued by Thornbury Town Council. I understand that compliance with this policy is essential to protecting the Council's information systems, data integrity, and legal obligations.

By signing this declaration, I agree to:

- Fully comply with all terms and conditions set out in the policy, including those relating to the use, care, and security of IT equipment and systems.
- Uphold the Council's standards for data protection, confidentiality, and responsible digital communication.
- Take personal responsibility for safeguarding Council data, whether accessed on Council-issued devices or personal devices under a BYOD arrangement.
- Participate in required training and remain informed of updates to this policy or related procedures.
- Acknowledge that non-compliance may result in disciplinary action, withdrawal of IT access or escalation under the Code of Conduct.

☐ I will use Council-issued IT equipment only
☐ I intend to use my personal device(s) under the Bring Your Own Device (BYOD) arrangement

---

If using Council-issued equipment, I further agree to:

- Use Council-provided devices exclusively for official Council business.
- Maintain strong security practices, including password protection and regular software updates.
- Enable and use Microsoft Two-Factor Authentication (2FA) on all relevant accounts.
- Permit device management through the Council's Mobile Device Management (MDM) system.
- Promptly report any loss, theft, or suspected data breach.

If using BYOD, I additionally agree to:

- Ensure the device meets all Council-mandated security requirements.
- Access Council systems only via approved methods and refrain from storing Council data locally.
- Maintain up-to-date antivirus protection and operating system updates.

- Cooperate with Officers if a data access request, FOI request, or security review is required.

Acknowledgement of Related Policies

I understand this policy operates in conjunction with the Council's Data Protection Policy, Freedom of Information Policy, Communications Policy, Code of Conduct, Training and Development Policy and other relevant governance documents. I agree to remain aware of and comply with these policies as part of my role.

Issued Equipment Details *(Complete if applicable)*

Device Type(s): _____

Make/Model: _____

Serial Number(s): _____

Accessories (e.g., keyboard, mouse, case): _____

Date of Issue: _____

Condition on Issue: _____

Councillor Details

Full Name: _____

Signature: _____

Date: _____

Council Officer Witness

Full Name: _____

Signature: _____

Date: _____