CHILTON TOWN COUNCIL

IT POLICY

DOCUMENT CONTROL	
Version Number	V1-2026
Adopted on	10 March 2026
Next Review	May 2028

Chilton Town Council

IT Policy

Introduction

Chilton Town Council values secure and effective IT and email use. This policy outlines the responsibilities of Councillors, staff, volunteers, and contractors in using Council IT systems.

Scope

This policy applies to all individuals who use the Council's IT resources, including computers, networks, software, devices, mobile phones, data, and email accounts. It applies regardless of working location or pattern.

The policy sets out expectations for appropriate use and provides that all users have (appropriate) responsibility for the safety and security of Chilton Town Council's IT systems and devices.

Acceptable use of IT resources, internet and email

Council IT systems, resources and devices are provided for official business. Limited personal use is permitted where reasonable and not disruptive.

Reasonable personal use of IT resources is defined as short, occasional, and non-disruptive activity that occurs primarily during breaks or outside of core working hours. It must not interfere with productivity, incur significant costs, or compromise Council policies or data security.

Examples of reasonable use include:

- **Brief Internet Browsing:** Quickly checking personal news, weather, or websites during lunch breaks or approved rest periods.
- **Checking Personal Email:** Briefly logging into personal webmail to check messages, provided it does not involve downloading large attachments or excessive time.
- **Essential Personal Communication:** Making quick phone calls or sending short messages, such as notifying family of running late or handling urgent domestic matters.
- **Online Banking/Shopping:** Accessing banking apps or making purchases during a lunch break.
- **Using Company Mobile for Non-Work Calls:** Making brief personal phone calls on a work-allocated phone.
- **Using Company Wi-Fi for Personal Devices:** Connecting a personal phone to the office Wi-Fi, provided it is permitted and does not violate data security policies.

Core Conditions for "Reasonable" must be minimal and not occur during "core" working hours.

- **Cost:** Does not cause additional financial costs to the employer.
- **Performance:** Does not slow down the network or decrease employee productivity.
- **Content:** Does not involve accessing illicit, offensive, or inappropriate material.
- **Security:** Does not involve installing unauthorized software or using unsecured networks.

Examples of *Unreasonable* Personal Use:

- Streaming music or movies.
- Online gaming or heavy, continuous browsing.
- Running a personal business using company equipment.
- Accessing social media sites during working hours.
- Storing personal photos or music files on company drive.

Users must not access illegal, inappropriate or unethical content and must comply with copyright law.

Photographs should only be taken where appropriate and with awareness of purpose. Private meetings or conversations must not be recorded without consent (subject to the legal framework for Council meetings).

Device and software use

Where possible, authorised devices, software, and applications will be provided by Chilton Town Council for work-related tasks. Installing personal or unauthorised software on such devices is prohibited. Personal USB sticks, discs of any kind, data storage devices etc cannot be used on Council computers without the prior approval of the Clerk.

Computers should be locked before leaving a desk, to prevent unauthorised access. All computers and devices supplied should be treated with good care at all times. Equipment should not be dismantled or reassembled without seeking advice.

If an item of portable equipment is lost or damaged this should be reported to the Clerk (or in the case of the Clerk, the Chair).

All users should note that all council data belongs to the council, which has data protection responsibilities, and must be treated accordingly by all users.

Data management and security

Confidential information must be stored and transmitted securely. Devices must be password or PIN protected, with encryption and multi-factor authentication used where appropriate.

Data should be backed up as necessary and securely destroyed when no longer required.

Email communication

Council emails must be used professionally and only for official matters. Sensitive content should be encrypted, e.g. with a password. Users must be cautious with attachments and links, and verify sources before opening.

Password and account security

Users are responsible for maintaining the security of their accounts and passwords; passwords should be strong and not shared with others. Regular password changes are encouraged.

Mobile devices and remote work

Council mobile devices must be secured with passcodes and/or biometrics. When working remotely, users should follow the same security standards as they would follow in the workplace.

Monitoring of IT Use and Email

As an IT provider, the council has the right to monitor the use of its IT equipment, systems and accounts including email, provided there is a legitimate reason for doing so and councillors, employees and any other users are informed, through this policy, that such monitoring may take place. Any monitoring must be proportionate and comply with relevant data protection and privacy laws.

Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements and Council policies.

Reporting security incidents

Any IT or email security issues must be reported immediately to the Town Clerk or, for urgent issues, the contracted IT Administrator.

Training and awareness

The Council will provide guidance and where needed training on IT security and email best practices.

Compliance and consequences

Breach of this IT and email policy may result in the suspension or loss of IT privileges and further consequences as deemed appropriate.