# Tendring Parish Council

# ICT Policy

This policy was approved at Full Council on the 28th July 2025.

## 1. Introduction

This Information and Communications Technology (ICT) Policy sets out how Tendring Parish Council manages and uses ICT resources to support its activities, ensure the security of information, and maintain public trust. It applies to all councillors and staff who use ICT systems on behalf of the council.

## 2. Purpose

The purpose of this policy is to:

- Ensure efficient, secure, and lawful use of ICT systems and data.
- Protect the integrity and security of council information.
- Support the delivery of services through effective use of technology.
- Set clear responsibilities for ICT use and data protection.

## 3. Scope

This policy applies to:

- All ICT equipment owned or used by the council, including computers, laptops, tablets, mobile phones, and storage devices.
- All software and online services used for council business.
- Use of council email, websites, social media, and cloud services.
- Personal devices when used to access council data or systems.

## 4. ICT Usage

### 4.1 Acceptable Use

- Council ICT systems must only be used for council-related activities.
- Personal use is permitted only where explicitly authorised and does not interfere with council operations or violate this policy.
- All users must act professionally and responsibly online.

### 4.2 Prohibited Use

- Accessing, creating, or transmitting offensive, illegal, or inappropriate content.
- Downloading unauthorised software or files that may harm systems or breach licensing.
- Using council systems for personal business, political campaigns, or commercial gain.

## 5. Data Protection and Security

### 5.1 Confidentiality

- Users must handle all council data in accordance with the UK General Data Protection Regulation (GDPR) and Data Protection Act 2018.
- Confidential or personal information must be stored securely and not shared without authorisation.

### 5.2 Passwords and Access

- Users must use strong passwords and change them regularly.
- Passwords must not be shared.
- Access to systems and data is granted based on job role and reviewed periodically.

### 5.3 Backups

- Data must be backed up regularly and securely.
- Cloud storage must meet UK data residency and security standards.

### 5.4 Device Security

- All devices must be protected with passwords.
- Users must report lost or stolen devices immediately to the Parish Clerk.

## 6. Email and Internet Use

- Council email addresses must be used for all official communications.
- Users should not click on suspicious links or open unexpected attachments.
- Internet access must be used responsibly and not for unlawful purposes.

## 7. Social Media and Website Management

- Only authorised individuals may post on the council's website.
- Content must be accurate, respectful, and relevant to council business.

- Comments or messages requiring a response should be directed to the Clerk or (where appropriate) responsible councillor.

**8. Software and Licensing**

- Only approved and licensed software may be installed or used.
- Users must not bypass software controls or use pirated content.

**9. Training and Awareness**

- All users should complete basic ICT and data protection training as required.
- Ongoing training may be provided to maintain awareness of threats such as phishing and malware.

**10. Monitoring and Audit**

- The council reserves the right to monitor ICT usage to ensure compliance.
- Audits may be conducted periodically to check for misuse or security risks.

**11. Breaches and Disciplinary Action**

- Breaches of this policy will be investigated and could result in disciplinary action.
- Serious breaches (e.g., data theft, illegal activity) may be reported to the relevant authority.

**12. Review and Amendments**

This policy will be reviewed regularly or when significant changes to technology, legislation, or council procedures occur.

Date of Approval: 28th July 2025
Date of Review: July 2028 or as required