

Information Technology Policy

1. Purpose

The purpose of this policy is to ensure the safe, secure, and effective use of information technology (IT) systems, services, and data by all members, employees, and contractors of the Parish Council. This policy sets out guidelines to protect the Council's digital assets and ensure compliance with relevant legislation.

2. Scope

This policy applies to:

- Councillors and staff (employees, contractors, volunteers)
- All IT equipment used during Parish Council business (including laptops, desktops, smartphones, tablets)
- All software, email, internet services, and cloud services used for council work

3. Acceptable Use

- IT equipment and services must be used primarily for Parish Council business.
- Limited personal use is permitted if it does not interfere with work duties, consume excessive resources, or breach any policies.
- Users must not access, store, or transmit material that is illegal, offensive, or discriminatory.

4. Passwords and Access

- Users must use strong passwords and change them regularly.
- Passwords must not be shared or written down in accessible locations.
- Access to council systems should be restricted based on role and necessity.

5. Data Protection and Confidentiality

- All users must comply with the UK GDPR and Data Protection Act 2018.
- Personal data must be stored securely and only shared with authorised individuals.
- Confidential council information must not be disclosed without proper authorisation.

6. Email and Communication

- Parish Council email accounts must be used for official communication.
- Email should be used professionally and with care, especially when handling sensitive or confidential information.

- Users should be wary of phishing emails and report suspicious messages.

7. Internet Usage

- Internet access is provided for council business and must be used responsibly.
- Downloading of unauthorised or pirated software is strictly prohibited.
- Users must not use council systems to access or distribute inappropriate content.

8. Software and Updates

- Only approved software may be installed on Parish Council devices.
- All devices must have up-to-date antivirus and software patches.
- Users must not disable or alter security settings without permission.

9. Use of Personal Devices (BYOD)

- Personal devices used for council business must meet minimum security standards (e.g. password protection, encryption).
- Council data must be stored separately and deleted when no longer needed or upon leaving the council.

10. Equipment Management

- All council-owned IT equipment remains the property of the Parish Council.
- Equipment must be returned upon leaving the council or on request.
- Loss or damage to devices must be reported immediately.

11. Backups and Records

- Important council data must be regularly backed up to secure locations.
- Electronic records should be managed in line with the Council's Records Management Policy.

12. Breaches and Enforcement

- Breaches of this policy may result in disciplinary action or removal of IT privileges.
- Serious breaches may be reported to external authorities if necessary.

13. Policy Review

This policy will be reviewed in response to changes in legislation or council requirements.

Next Review Due:	May 2027
Reviewed:	13 th October 2026
Adopted at Full Council meeting:	6th May 2025