Weston Turville
Parish Council

IT Policy

Version Control

Review Date	Version no	Amendment
19 June 2025	1	Policy adopted

1. Purpose

This policy provides guidance on the acceptable and secure use of IT systems, data, and digital resources used by Weston Turville Parish Council. It ensures that council operations are carried out efficiently, securely, and in compliance with legal obligations.

2. Scope

This policy applies to all parish councillors, staff, volunteers, and contractors who use or have access to the Council's IT systems, including:

- Computers, laptops, tablets, and smartphones
- Council email accounts and cloud services
- Internet and network access
- Data storage and communication tools

3. Software and Licensing

- Only licensed software approved by the Council may be used.
- Users must not copy, share, or install software without permission.

4. Website Management and Accessibility

- The Parish Council website must meet WCAG 2.2AA standards and publish all required documents, including minutes, AGARs, councillor details.

5. Hardware Maintenance and Replacement

- All IT hardware (e.g. computers, laptops, printers) will be reviewed regularly to ensure it is fit for purpose and secure.
- Devices will typically be replaced every 3 to 5 years, or sooner if performance, security, or support issues arise.
- Obsolete or faulty hardware must be securely disposed of in line with data protection regulations and offered to local organisations or individuals at an agreed price.
- The Clerk will maintain an inventory of council IT equipment and oversee replacement planning.

6. Acceptable Use

Users must:

- Use council IT resources only for official council business.
- Keep login credentials confidential.
- Ensure devices are locked when unattended.
- Report any lost or stolen devices immediately.

Users must not:

- Use council equipment for personal gain or political purposes.
- Access, download, or distribute inappropriate or illegal material.
- Install unauthorized software or applications.

7. Email and Communications

- Council email accounts must be used for all council business.
- Communications must be respectful and professional.
- Email attachments should be scanned for viruses before opening

8. Security

- Devices must have up-to-date antivirus and system updates.
- Passwords must be strong and changed regularly.
- Two-factor authentication should be used where available.
- Regular backups must be performed for important data.

9. Social Media and Communications

- Please refer the Council’s Social Media policy.

10. Data Protection & Confidentiality

All users must:

- Follow the UK GDPR and Data Protection Act 2018.
- Store and process personal data securely.
- Not share personal data without proper authority.
- Use council-provided cloud storage or email for official correspondence (not personal email accounts).
- Sensitive data must not be stored on unencrypted personal devices.

11. Breach and Incident Reporting

All security breaches or suspected data breaches must be reported immediately to the Clerk. An incident log will be maintained, and necessary actions will be taken, including notifying the ICO where required.

12. Review and Amendments

This policy will be reviewed annually or as needed due to changes in legislation or council operations.