Waldridge Parish Council IT Policy

1. Purpose

This policy sets out how the Parish Council manages, secures, and uses its information technology systems to ensure reliable operations, protect data, and comply with legal and regulatory obligations.

2. Scope

This policy applies to all councillors, employees, contractors, and volunteers who access or use Parish Council IT systems, devices, networks, or data.

3. Roles and Responsibilities

- **Clerk/Responsible Officer** — Oversees IT systems, ensures compliance, manages access permissions, and coordinates with external IT providers.
- **Councillors and Staff** — Follow this policy, report incidents promptly, and use IT resources responsibly.
- **External Providers** — Must comply with data protection and security requirements outlined in contracts.

4. Acceptable Use

- IT systems must be used for legitimate Parish Council business.
- Personal use is permitted only when minimal, lawful, and not disruptive.
- Users must not install unauthorised software or connect unapproved devices.
- Access credentials must not be shared.

5. Data Protection and Privacy

- Personal data must be processed in accordance with UK GDPR and the Data Protection Act 2018.
- Only authorised individuals may access personal or sensitive data.
- Data must be stored securely using approved systems.
- Email containing personal data must be encrypted or password-protected when appropriate.

6. Information Security

- All devices must be protected with strong passwords and, where possible, multi-factor authentication.
- Antivirus and security updates must be enabled and kept current.

- Users must lock screens when leaving devices unattended.
- Public Wi-Fi must not be used for accessing sensitive information unless a secure VPN is used.

7. Email and Communication

- Parish Council email accounts must be used for all official correspondence.
- Users must be vigilant about phishing and suspicious messages.
- Bulk emails must use appropriate safeguards such as BCC to protect personal data.

8. Remote Working

- Remote access must use approved devices and secure connections.
- Confidential documents must not be stored on personal devices unless authorised and protected.

9. Social Media and Website Management

- Only authorised individuals may post on official Parish Council platforms.
- Content must be factual, respectful, and compliant with council policies.
- Personal opinions must not be presented as council positions.

10. Procurement and Asset Management

- All IT equipment purchases must be approved by the Clerk or Council.
- An asset register must be maintained for all devices.
- Devices must be returned when a user leaves their role.

11. Backup and Data Retention

- Data must be backed up regularly using approved systems.
- Retention periods must follow the Council's Records Management Policy.
- Obsolete data must be securely deleted.

12. Incident Reporting and Response

- Users must report suspected data breaches, cyber incidents, or equipment loss immediately.
- The Clerk will coordinate investigation and reporting, including notifying the ICO when required.

13. Training and Awareness

- All users must complete periodic training on cybersecurity, data protection, and IT best practices.

14. Policy Review

This policy will be reviewed annually or sooner if legislation, technology, or operational needs change.

Date of adoption: 10.3.26 at Parish Meeting

Date for next review: March 2027