Woodbury Parish Council

(serving Exton, Woodbury, and Woodbury Salterton)

Information Technology (IT) / Data Security Policy

1. Introduction and Purpose

This policy establishes the rules for the secure and appropriate use of Woodbury Parish Council's information technology (IT) systems and data. Its purpose is to:

- Ensure all Users understand their responsibilities.
- Protect the Council's IT equipment, systems, and data from loss, misuse, or theft.
- Safeguard the privacy of councillors, employees, parishioners and third parties.
- Ensure compliance with relevant UK legislation, including data protection, freedom of information, and accessibility laws.

This policy is a key part of the Council's risk management and serves as our primary defence against IT-related incidents such as data breaches, cyber-attacks, and legal non-compliance.

2. Definitions

- **Users:** All councillors, employees, contractors, and volunteers acting on behalf of the Council as well as third parties.
- **Data:** Any digitally stored information, including but not limited to documents, emails, copyrighted material, images, personal data, and financial records.
- **IT Systems:** All council-owned or managed hardware and software, including computers, laptops, mobile phones, servers, internet access, email accounts, cloud storage, and the Council website.

3. Scope

This policy applies to all **Users** and covers the use of all **IT Systems**, whether accessed on council premises, remotely, or from personal devices when used for council business.

4. Acceptable Use of IT Systems

- **Council Business Only:** IT systems are provided for official council business only. Personal use is strictly prohibited.
- **Authorised Use:** Users must not access data or software they are not authorised to use. Unauthorised changes to systems or data are forbidden.
- **Software:** Users must not install unauthorised software on council equipment. Clarification on approved software can be sought from the Clerk.

- **Return of Equipment:** All council equipment must be returned to the Clerk, Chairman, or Vice-Chairman upon the end of a term of office, employment, or contract. A charge may be levied for lost or damaged equipment.

5. Council Email and Communication

- **Official Email Address:** The Council will provide an official email address (e.g., `name@woodburyparishcouncil.gov.uk`) to all councillors and employees. **This must be used for all council correspondence, both official and unofficial.**
- **No Personal Email for Business:** To prevent **lost emails when personnel change**, Users are prohibited from using personal email accounts (e.g., Gmail, Hotmail) for council business.
- **Email Footers:** An appropriate official footer, provided by the Clerk, must be added to all outgoing emails.
- **Record Keeping:** Any correspondence undertaken on behalf of the Council (on council or personal devices) is a council record and must be provided to the Clerk upon request, especially in relation to Freedom of Information (FOI) requests. It is good practice that the Clerk is CC'd BC'd in all correspondence.

6. Data Protection and Information Security

Users must adhere to the Council's Data Protection Policy and Document Retention Policy at all times.

- **Data Sharing:** Council data or software must not be transferred to any external person or organisation without proper authority.
- **Secure Storage:** Data must be stored and accessed only via council-approved, secure methods. Personal data must not be stored on unencrypted USB sticks, personal cloud services, or personal devices unless explicitly authorised.
- **Preventing Data Breaches:** To prevent data breaches from unsecured channels, Users must:
    - Never leave a logged-in account unattended on an unlocked device.
    - Use strong passwords and multi-factor authentication where available (see Section 7).
    - Immediately report any suspected **loss or theft of data** (e.g., a lost laptop or an email sent to the wrong recipient) to the Clerk and Chairman.

7. Passwords and Access Control

- **Password Strength:** Passwords must be either:
    - A minimum of 20 random characters (ideally 25+), or
    - A passphrase of four or five random words separated by non-alphanumeric characters.
- **Two-Factor Authentication (2FA):** Where available, 2FA **must** be enabled, using a hardware key or an authenticator app (e.g., Google Authenticator).
- **Password Log:** For business continuity, essential passwords must be securely logged with the Clerk.
- **Biometric Authentication:** On council-provided devices, biometric authentication (e.g., fingerprint, facial recognition) should be activated under a council-managed account.

8. Website Management and Legal Compliance

The Council website is a critical public-facing system and must be managed professionally.

- **Accessibility:** The website **must** meet WCAG 2.2 AA standards to comply with **The Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018**. Responsibility for regular accessibility and broken link checks will be assigned by the Council.
- **Transparency:** All required documents (minutes, agendas, financial information, councillor details) must be published promptly in accordance with the Transparency Code.
- **FOI Requests:** Freedom of Information requests received via the website or any other channel must be handled in accordance with the Council's FOI procedure and legal timelines.

9. Cybersecurity and Risk Management

The Council will take proactive steps to defend against **cyber attacks** such as phishing and malware.

- **Insurance and Security:** Equipment is insured, but Users must take practical steps to secure it from theft or unauthorised use. Devices must not be left in unattended vehicles unless absolutely necessary and must be secured out of sight.
- **Incident Reporting:** Any loss, damage, or criminal activity involving IT equipment must be reported immediately to the Clerk and Chairman.

- **Vigilance:** Users must be vigilant against suspicious emails (**phishing**). Do not click links or open attachments from unknown senders. Suspected phishing attempts must be reported to the Clerk.
- **Annual Risk Assessment:** An annual risk assessment of the Council's IT hardware, software, and data security will be conducted.

10. Social Media and Online Conduct

- **Official Accounts:** Only authorised personnel may post on the Council's official social media accounts.
- **Personal Accounts:** Councillors and staff must make it clear when expressing personal views online that they are not speaking on behalf of the Council. Professional conduct is expected at all times.

11. Policy Review and Training

- **Review Cycle:** This policy will be reviewed **annually**, or upon a significant change in IT systems or legislation. A review will also be triggered within three months of new staff starting or following council elections.
- **Training:** All Users will receive periodic training on this policy, data protection, and IT security best practices to ensure ongoing compliance and awareness.

Originally adopted : 13th May 2024

Updated: 27th October 2025

Reviewed: Annually