Woodham Mortimer and Hazeleigh Parish Council

Information Technology (IT) Policy

1. Introduction

This IT Policy outlines the principles and procedures governing the use of information technology by Woodham Mortimer and Hazeleigh Parish Council. It reflects the Council's size, limited budget, and current IT setup, where the Clerk is the sole employee using council-owned equipment and councilors use personal devices. The policy draws on best practices and is designed to ensure secure, responsible, and compliant use of IT resources.

2. Scope

This Policy applies to the Clerk, all Members (councilors), and any contractor or volunteer who is given access to Council data or systems. It covers all devices, accounts, and digital systems used for Council business, whether owned by the Council or by individuals.

3. Acceptable Use

All IT resources must be used ethically, responsibly, and in accordance with legal and regulatory requirements. Council-owned equipment is to be used solely for council business. Councillors using personal devices must ensure they access council data only through secure channels, maintain confidentiality and adhere to these basic principles:

- Council business must be conducted using council-issued email accounts
- Personal email accounts must not be used
- Council data must not be stored on personal cloud services

4. Email and Domain Governance

The Council owns and controls its official domain name and provides official email accounts for the Clerk and Members. All Council business must be conducted using these accounts. Forwarding Council emails to personal accounts should be avoided. The Clerk administers all accounts and ensures access is removed when Members leave office.

5. Device and Email Management

The Clerk uses a council-owned laptop for official duties. All councilors use personal devices to access council communications. Secure MS365 and Exchange accounts are administered by the Clerk to ensure data integrity and security. Multi-factor authentication (MFA) should be enabled on all Council email accounts. Councilors must ensure their personal devices used for Council business have device encryption enabled and do not store Council data locally unless explicitly authorised.

6. Website & Digital Compliance

The Council shall maintain a website that meets international accessibility standards for public sector websites. Required documents must be published in accordance with the Transparency Code. The website must be hosted on a secure platform appropriately backed up.

7. Data Protection

All users must comply with the UK General Data Protection Regulation (GDPR). Personal data must be handled securely and only for legitimate council purposes. The Clerk is responsible for maintaining data protection protocols and ensuring that councilors are aware of their responsibilities. Digital records must be retained and disposed of in accordance with the Council polices. All Freedom of Information (FOI) and Subject Access Requests (SARs) must be handled using Council-controlled systems to ensure information is retrievable.

8. Cybersecurity

Basic cybersecurity measures must be followed by all users. These include using strong passwords, enabling device encryption, installing software updates promptly, and avoiding suspicious links or attachments. The Clerk will monitor and maintain antivirus protection on the council-owned laptop.

9. Remote Working

The Clerk may work remotely using the council-owned laptop. Remote access must be secure and comply with data protection and cybersecurity standards. Councilors accessing council data remotely must do so via secure MS365 accounts and follow these security policies.

10. Councilor Responsibilities

Councilors must ensure their personal devices used for council business are secure. This includes:

- Using strong passwords
- Enabling device encryption
- Keeping software up to date
- Reporting any suspected data breaches or device loss to the Clerk immediately
- No use of WhatsApp, SMS, or social media for council business.

11. Breach Reporting

Any suspected data breach, cybersecurity incident, or loss of a device containing Council data must be reported to the Clerk immediately. The Clerk will assess the incident and, where required, report it to the Council and the ICO

12. Policy Review

This policy will be reviewed annually or as required to reflect changes in technology, legislation, council operations or requirements of the Small Authorities Proper Practices Panel (SAPPP). It should be read in conjunction with the Council's Standing Orders, Financial Regulations, and Press and Media Policy.

..... *Simon Brady*..... (Simon Brady Chairman to the Council) 14/04/2026