Fenny Compton Parish Council IT Policy

1. Aims

This policy sets out how the Parish Council will use and manage its IT systems and information. It aims to:

- Protect council data and equipment.
- Support councillors and staff in carrying out their roles.
- Ensure compliance with relevant laws, including data protection.

2. Scope

This policy applies to:

- All councillors and staff who use parish council computers, email accounts, cloud storage, or other IT resources.
- Any personal devices used for council business (e.g. laptops, tablets, or phones).

3. Acceptable Use

- Parish Council IT systems and accounts must only be used for council business.
- Personal use of council-provided equipment should be minimal and must not interfere with council work.
- Inappropriate, offensive or unlawful activity is strictly prohibited.

4. Data Protection and Confidentiality

- Councillors and staff must handle all personal data in line with UK GDPR and the Data Protection Act.
- Councillors and staff must comply with the Data Protection Policy.
- Confidential information must not be shared outside the council unless authorised.
- Personal devices used for council business must be secured with a password or PIN.

5. Email and Communication

- Council email accounts should be used for all council business.
- Emails must be written professionally and treated as public records.

- Care must be taken not to open suspicious links or attachments.

6. Security

- Strong passwords must be used and changed regularly.
- Devices must be locked when unattended.
- Antivirus and software updates must be kept up to date.
- Cloud services or online storage must be approved by the council.

7. Social Media and Website

- Only authorised councillors or staff may post on the council's website or social media accounts.
- Posts must reflect official council decisions and maintain a professional tone.
- Personal opinions should not be posted from council accounts.

8. Backup and Records

- Important council documents must be stored in the official shared drive or approved system.
- Regular backups must be taken to prevent data loss.
- Records must be retained and disposed of in line with the Council's Document Retention Policy.

9. Breaches and Reporting

- Any suspected IT security breach (e.g. lost device, data leak, hacking attempt) must be reported to the Clerk immediately.
- The council will investigate breaches and take appropriate action.

10. Review

This policy will be reviewed every three years or when significant changes in technology or legislation occur.