Shimpling Parish Council

Information Technology (IT) and Acceptable Use Policy

- **1. Purpose**

This policy sets out how Shimpling Parish Council manages and uses its IT systems, email accounts, devices, and data. It ensures compliance with data protection legislation and promotes secure, responsible use of technology by the Clerk and Councillors.

- **2. Scope**

This policy applies to:

- The Clerk
- All Parish Councillors
- Any contractors or volunteers given access to council IT systems

It covers:

- Email accounts (@shimpling-pc.gov.uk)
- Devices used for council business
- Storage and sharing of council information

- **3. Email Use**
- **3.1 Official Email Accounts**

- The Clerk will use: clerk@shimpling-pc.gov.uk
- Councillors will use: [initials]@shimpling-pc.gov.uk
- These accounts must be used for all council-related correspondence.

- **3.2 Acceptable Use**

Users must:

- Use professional and respectful language
- Keep personal and council emails separate
- Not use council email for political campaigning or personal business

- **3.3 Security**

- Strong passwords must be used and not shared
- Two-factor authentication should be enabled where possible
- Suspicious emails (e.g. phishing) must not be opened and should be reported to the Clerk

- **4. Devices and Access**
- **4.1 Approved Devices**

- Council business may be conducted on council-owned or personal devices
- Personal devices must have:
  - Up-to-date antivirus software
  - Operating system updates enabled
  - Password or biometric protection

- **4.2 Public or Shared Devices**

- Council systems must not be accessed on public/shared computers

- **5. Data Protection and Storage**
- **5.1 Handling Information**

  - Personal data must be handled in accordance with UK GDPR
  - Only collect and retain necessary information

- **5.2 Storage**

  - Council documents should be stored in an approved shared location (e.g. secure cloud storage)
  - Sensitive information must not be stored locally unless necessary

- **5.3 Retention**

  - Documents must be retained and deleted in line with the council's retention policy

- **6. Information Sharing**

  - Personal data must only be shared where there is a lawful basis
  - Emails containing personal data should be sent securely
  - Group emails must use BCC where appropriate

- **7. Website and Social Media**

  - Only authorised individuals may post on behalf of the council
  - Content must be accurate, lawful, and not defamatory

- **8. Incident Management**

Any of the following must be reported immediately to the Clerk:

- Data breaches or suspected breaches
- Lost or stolen devices used for council business
- Unauthorised access to council systems

The Clerk will assess whether the incident must be reported to the Information Commissioner's Office (ICO).

- **9. Backup and Continuity**

- Important council data must be regularly backed up
- Access to key systems should not rely on a single individual

- **10. Training and Awareness**

- The Clerk and Councillors should undertake periodic training on:
  - Data protection
  - Cyber security

- **11. Monitoring and Compliance**

- The Council reserves the right to monitor use of its IT systems for compliance
- Misuse may result in action under the council's code of conduct

- **12. Review**

This policy will be reviewed annually or following significant changes to legislation or council systems.

Adopted by Shimpling Parish Council
Signed: Natasha Byford (Clerk and RFO)
Date: 11th May 2026