SITHNEY PARISH COUNCIL

Information Technology (IT) Policy

1. **Aim -** This policy sets out the principles, responsibilities, and acceptable use of Information Technology (IT) resources by Sithney Parish Council ("the Council"). Its aim is to ensure secure, lawful, and efficient use of IT systems, safeguarding the Council's information, assets, and reputation.
2. **Scope –**
    - This policy applies to All Councillors, employees, contractors, and volunteers using Council IT systems or accessing Council data.
    - All Council-owned devices, software, cloud systems, and communication platforms.
    - Personal devices used to access Council data ("Bring Your Own Device", BYOD).

3. Legal and Regulatory Compliance

The Council shall comply with all relevant legislation and guidance, including:

- Data Protection Act 2018 and UK GDPR
- Freedom of Information Act 2000
- Local Government Act 1972 and related statutes
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Public Records Act 1958
- NCSC (National Cyber Security Centre) guidance where applicable

4. Responsibilities

- **Clerk/Responsible Officer**: Oversees compliance, security, and policy implementation.
- **Councillors**: Must follow this policy and report breaches or incidents promptly.
- **IT Providers/Contractors**: Must adhere to Council standards and maintain confidentiality.

5. Acceptable Use - General Principles

- IT resources are provided for official Council business. Limited personal use is permitted if it does not interfere with Council operations or breach this policy.
- Users must not:
    - Access, transmit, or store offensive, unlawful, or defamatory material.
    - Use Council IT for political campaigning, personal business, or profit-making activities.
    - Install unauthorised software or alter system configurations.

Email and Communication

- Council email addresses must be used for official Council business.
- The council uses ***.gov.uk*** e-mail address for councillors and the clerk / RFO.
- Emails and electronic communications may be subject to disclosure under Freedom of Information legislation.
- Councillors and the clerk / RFO must always use professional and respectful language.

6. Data Protection and Confidentiality

- All personal data must be processed in accordance with the Council's Data Protection Policy.
- Council documents must be stored in secure systems approved by the Council.
- Confidential or sensitive data must not be stored on unencrypted personal devices.
- USB drives or portable media should be avoided; if used, they must be encrypted.

7. Security Measures

- Strong passwords (minimum 12 characters, mix of letters, numbers, symbols) must be used.
- Multi-Factor Authentication (MFA) shall be enabled where available.
- Devices must be kept updated with security patches and antivirus software.
- Lost or stolen devices must be reported immediately to the Full Council.
- Remote access must be via secure connections only.
- Passwords not to be shared.

8. Social Media and Online Presence

- Councillors and staff must not post confidential information or represent personal views as Council policy.

9. Monitoring and Audit

- The Council reserves the right to monitor use of IT systems to ensure compliance, subject to lawful safeguards.
- Breaches of this policy may result in disciplinary action, referral to external authorities, or legal proceedings.

10. Incident Reporting

- All suspected IT security breaches, data losses, or cyber incidents must be reported immediately to the Clerk.
- Where a personal data breach occurs, the Clerk will assess and, if necessary, report to the ICO within 72 hours.

11. Policy Review

This policy will be reviewed every two years or sooner if legislation, technology, or the Council needs to change something.

Adopted 4th November 2025