St Michael Penkivel Parish Council

St Michael Penkivel Parish Council Information Technology (IT) Policy

1. Purpose

This policy defines how St Michael Penkivel Parish Council manages its use of information technology, in line with the Transparency Code for Smaller Authorities (2015) and the 2025 edition of the Practitioners' Guide. It ensures the council's digital operations are transparent, secure, and compliant with data protection laws.

2. Scope

This policy applies to all councillors, employees, volunteers and contractors who use or manage the council's IT resources, including, but not limited to:

- Desktop and laptop computers, tablets and smartphones
- Email and cloud-based systems
- Council website
- Video conferencing and messaging platforms
- Personal devices used for council business

3. Governance and Oversight The Clerk is the Data Protection Officer (DPO) and IT administrator.

4. Data Protection and Security

All processing of personal data shall comply with the UK Data Protection Regulation (UKGDPR) and Data Protection Act 2018.

Privacy Policy: All data collection, processing, and subject rights are governed by the council's Privacy Policy, available from the Clerk.

Access and Storage: Data is secured securely by the Clerk, with access only granted to authorised personnel based on necessity.

Retention: Personal data will be retained in accordance with the council's Data Retention Schedule and securely deleted when no longer needed.

Security Controls:

- Strong password protection with multi-factor authentication where possible is required for all systems
- Passwords used on council systems are unique to this environment and no user must use logins associated with non-council systems
- Regular security updates and anti-malware software are required on all council-owned and personal devices
- Backups of essential data must be stored in a secure location

Access Controls: Should any personnel or member leave the council, the Clerk will rescind access to the council systems for the leaving person. This includes changing the password and freezing email accounts, access to council systems (accounting software, cloud storage, website admin).

5. Use of Personal Devices

Staff may use personal devices for council business only if explicitly authorised and subject to compliance with this policy.

Councillors staff may use personal devices for council business and subject to compliance with this policy. This includes the use of council-owned domain-based email.

Devices must be protected with strong passwords, encryption (where possible) and up to date antivirus software.

Council data must be kept separate from personal data using dedicated apps or storage area.

6. Use of Personal Email Addresses

The use of personal email accounts for council business is not best practise. All council correspondence should be conducted through official council-provided email addresses. Council emails must not be shared or forwarded outside of approved data areas.

Monitoring and Compliance: Any breaches will be investigated and appropriate measures taken in line with the council's disciplinary or grievance procedures.

Email retention: All council emails must be stored in compliance with the GDPR, DPA and Freedom of Information requirements.

All councillors using council-owned email systems should ensure the Clerk is copied in to all correspondence, including replies.

7. IT Infrastructure and Support

Asset Register: Maintained for all council owned hardware and software.

Maintenance: All devices must be regularly updated and checked for compliance with this policy along with recommended software updates and both strong password with multi-factor authentication enabled where possible.

Training: Users will be given training on IT systems, cybersecurity, data handling, and transparency responsibilities.

8. Data Breach Process and Protocols

The Parish Council is committed to responding promptly and effectively to any data breaches to minimise risk and comply with UK GDPR and DPA requirements.

9. Definition of a Data Breach

A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include

- Loss or theft of devices containing personal data
- Unauthorised access to council email accounts or files
- Sending personal data to the wrong recipient
- Malware or ransomware attacks compromising council systems

Reporting a breach

Immediate notification: Any councillor, employee or contractor who becomes aware of a data breach must report it immediately to the Clerk (Data Protection Officer)

Initial Response: The Clerk in consultation with the council will assess the severity and scope of the breach and determine if mitigation steps are required (eg changing passwords, disabling access).

Investigation: An investigation will be conducted by the Clerk within 72 hours of the breach being discovered. The breach will be logged, including

- Date and time of the breach
- Type and volume of data affected
- Cause and extent of the breach
- Actions taken to address the breach

Notification: If a breach is likely to result in the rights and freedoms of individuals, the council must notify the Information Commissioner' Office (ICO) within 72 hours.

If the breach poses a high risk to the individuals affected, those individuals must also be informed without undue delay, outlining

- The nature of the breach
- The likely consequences
- Measures taken to mitigate the risk
- Contact information for further support

Remediation and Review:

- The Clerk will ensure that lessons are learned, policies, procedures or training are updated as necessary
- Technical fixes or security upgrades will be prioritised to prevent recurrence
- Breach logs will be reviewed periodically to identify systemic issues

10. Review

This policy will be reviewed regularly, and will be subject to legislation changes.

This policy was adopted by St Michael Penkivel Parish Council on 11 March 2026.