Pennington Parish Council

IT Policy

Revised and re-adopted at the full council meeting on March 2025 New revision date 2026

1. Purpose and scope

This policy sets out how Pennington Parish Council manages its digital systems, data, and electronic communications.
It ensures that the Council complies with:

- Assertion 10 – *Digital and Data Compliance* (Practitioners' Guide 2025 for Smaller Authorities)
- The Data Protection Act 2018 and UK GDPR
- The Freedom of Information Act 2000
- The Public Sector Bodies (Websites and Mobile Applications) Accessibility Regulations 2018
- The Local Government Transparency Code 2015

This policy applies to all councillors, employees, contractors, and volunteers who access, process or store Council information using Council or personal devices.

2. Governance and responsibilities

- The Parish Clerk is the Council's Data Protection Lead and IT coordinator, responsible for day-to-day compliance and reporting to the Council
- All Councillors and staff must comply with this policy when handling Council data or using IT systems

3. Use of Council email and domain

- All official Council business must be conducted using the Council's authorised email domain: pennington-pc.gov.uk
- Personal email accounts (e.g. Gmail, Hotmail, Yahoo) **must not** be used for Council business
- Emails must be written professionally and stored in accordance with the Council's document-retention and data-protection policies
- Councillors and staff must regularly check their Council email and respond promptly

4. Data safety and protection

- Personal data must be collected, processed and stored lawfully and securely in accordance with the UK GDPR and Data Protection Act 2018
- Sensitive or confidential information must not be shared via unsecured channels
- Paper and digital records must be stored safely, with access limited to those who need it
- Council data must not be copied or shared with third parties unless authorised by the Clerk and/or Council resolution

5. Use of Council and personal devices

- The Council will provide devices (e.g., laptop, tablet) for official use to the Clerk as a minimum
- If personal devices (phones, tablets, laptops) are used for Council work:
    - They must be password-protected
    - They must have up-to-date antivirus software and operating systems
    - Council data must be stored separately from personal data

    - Data relating to Council business must be deleted when no longer required or when a councillor leaves office
- Public Wi-Fi should not be used for confidential work unless a secure VPN is used

6. Passwords and access control

- All devices and accounts must be secured with strong passwords (including upper/lower case, numbers, and symbols and must not use easily guessable combinations or duplicate passwords)
- Passwords must not be shared or written down in accessible places.
- Where available, multi-factor authentication (MFA) should be enabled
- Accounts must be locked or logged off when devices are left unattended

7. Data storage, back-ups and retention

- Council data shall be stored in secure, backed-up environments such as approved cloud storage (e.g., Microsoft 365, Google Workspace, or equivalent)
- Data must be backed up regularly (at least weekly) and tested periodically for recovery
- Backups must be encrypted and stored in compliance with the Council's retention schedule
- Data no longer required shall be deleted or archived securely in line with the Council's Retention and Disposal Policy

8. Encryption and security

- All laptops and portable devices must have full-disk encryption enabled where possible
- Files containing sensitive data should be password-protected or encrypted before being emailed or transferred
- USB drives or external media should be avoided; if used, they must be encrypted and stored securely
- Anti-virus and firewall protections must be active and up-to-date on all devices

9. Website, online services and accessibility

- The Council's website is managed under its control and complies with the Accessibility Regulations 2018 and WCAG 2.2 AA standard
- Personal data published online (such as councillor contact details) will be limited to what is necessary
- Only authorised users may update website content or online services
- The Council will ensure that web hosting and email providers meet security and GDPR compliance standards

10. Data breaches and incident response

If a data breach occurs (loss, theft, unauthorised disclosure, or access to personal data):

- The person discovering the breach must report it immediately to the Clerk
- The Clerk will assess the breach, contain the issue, and determine whether it must be reported to the Information Commissioner's Office (ICO) within 72 hours
- The Clerk will maintain a Data Breach Log
- Affected individuals will be informed promptly if there is a risk to their rights or freedoms
- The Council will review its systems and implement corrective measures

11. Training and awareness

- Councillors and staff will receive periodic training on data protection, cyber security, and digital compliance
- New members will receive an induction covering this policy
- The Clerk will keep training records for audit purposes

12. Third-party processors and suppliers

- Any external contractor or supplier handling Council data must provide written assurance of compliance with UK GDPR and this policy
- A Data Processing Agreement (DPA**)** must be in place before sharing data with third parties

13. Monitoring, review and audit

- The Council will review its IT, digital and data arrangements annually as part of its Annual Governance and Accountability Return (AGAR) process
- Findings will be recorded under Assertion 10: Digital and Data Compliance
- This policy will be reviewed annually or sooner if required by legislation, risk assessment, or internal audit findings