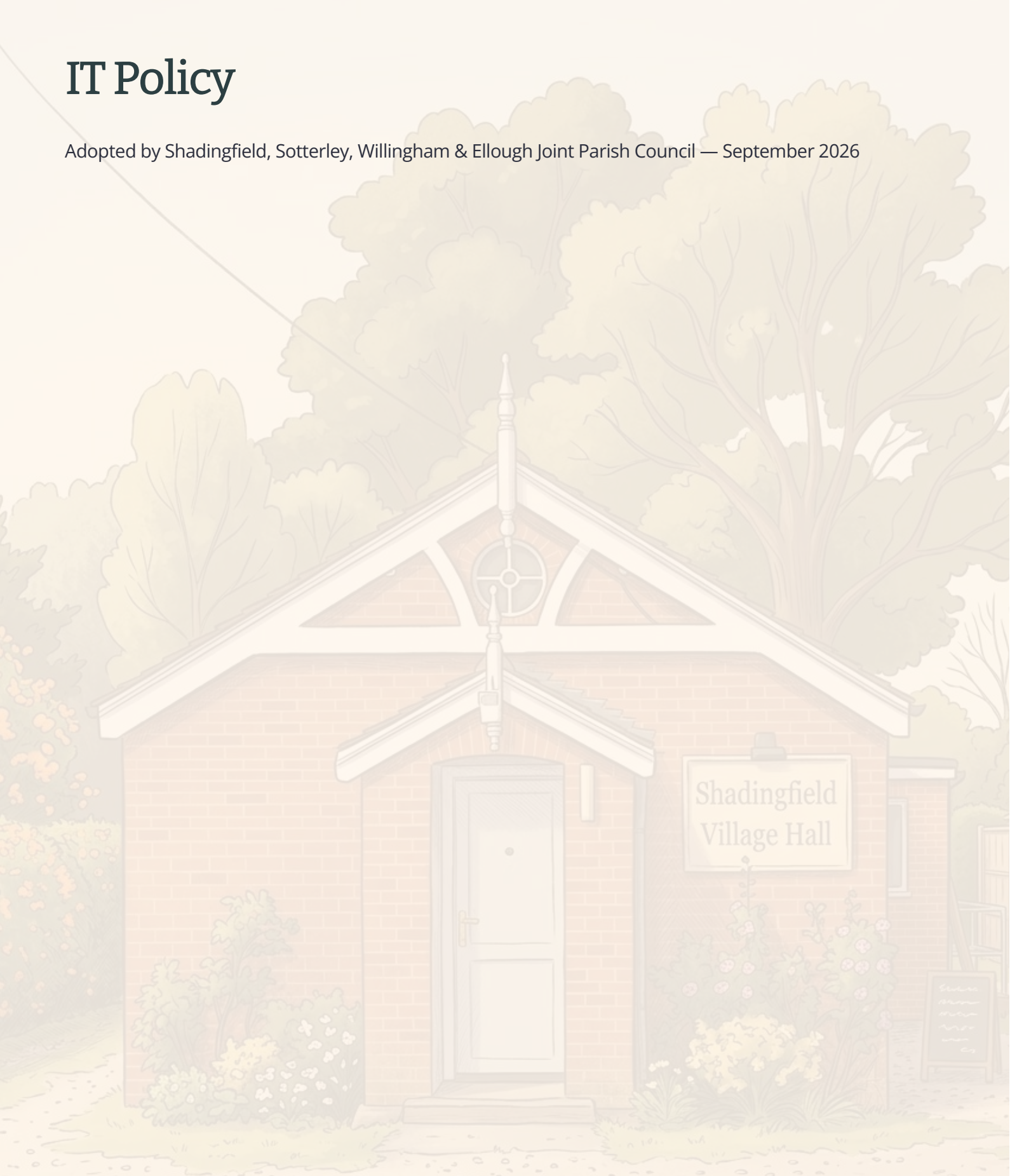
IT Policy

Adopted by Shadingfield, Sotterley, Willingham & Ellough Joint Parish Council — September 2026



Next review: September 2027

This policy will be reviewed annually, or sooner if required by changes in legislation, technology, or council operations.

Policy Statement

This policy sets the standards for the use of information technology, electronic communications, and email systems by councillors, employees, and authorised volunteers. Its purpose is to ensure that council information is handled securely, accountably, and lawfully.

Scope

This policy applies to:

- All councillors, employees, and authorised volunteers acting on behalf of the Council.
- All devices used to conduct council business, including council-owned and personal devices.
- All electronic communications, including email, messaging platforms, cloud storage, and document-sharing tools.

This policy should be read alongside the Council's Data Protection Policy, Data & Electronic Data Retention Policy, Social Media Policy, Home Working Policy, and Code of Conduct.

Use of Council IT Equipment

Council IT equipment and systems are provided for council business. Limited personal use of council equipment is permitted where it is reasonable, does not interfere with council duties, and does not put council information at risk.

Users must not install software on council-owned equipment without the Clerk's agreement.

Users must take reasonable care to prevent loss, theft, or damage to council equipment.

Council-owned equipment remains the property of the Council and must be returned when a person ceases to hold office or employment.

Data Storage and Backup

Council records must be stored in the Council's approved storage locations rather than solely on individual devices.

Council data must be backed up regularly so that records can be recovered if a device is lost, damaged, or fails. The Clerk is responsible for ensuring that backups are in place and working.

Equipment must be securely wiped before disposal.

Mandatory Use of Council Email Accounts

All official council business must be conducted using council email accounts on the Council's own domain, for example clerk@shadingfield-jpc.gov.uk. This includes:

- Correspondence with residents, contractors, partner organisations, and statutory bodies.
- Circulation of agendas, minutes, reports, and working papers.
- Communications relating to planning matters, finance, governance, and policy.
- Any discussion or exchange of information that forms part of the Council's decision-making or administrative processes.

Personal email accounts must not be used for council business.

Legal and Regulatory Compliance

Using council email accounts supports compliance with:

UK GDPR and the Data Protection Act 2018

Ensuring personal data is processed securely and appropriately.

The Freedom of Information Act 2000

Ensuring records are accessible when the Council receives a request.

The Council's Data & Electronic Data Retention Policy

Ensuring emails are retained, archived, and disposed of correctly.

Security and Access Control

Account Management

Council email accounts will be issued and managed by the Clerk.

Passwords

Passwords must be strong, unique to the account, and must not be shared. Passwords must be changed immediately if there is any reason to suspect they have been compromised.

Multi-factor Authentication

Multi-factor authentication must be enabled where available.

Access Sharing

Access to council email accounts must not be shared with any other person.

Use of Personal Devices

Where councillors, employees, or authorised volunteers use personal devices to access council email or council information:

- Devices must have up-to-date security updates and antivirus protection.
- Devices must be protected by a password, PIN, or biometric lock.
- Council information must not be stored permanently on personal devices unless authorised and protected.
- Council email accounts must only be accessed through a secure application or a secure web browser session.

Appropriate Use of Email

Users must:

- Communicate professionally and respectfully at all times.
- Ensure emails are factual, accurate, and suitable for public disclosure.
- Be cautious with attachments and links, and verify the sender before opening an attachment or following a link in an unexpected message.
- Avoid sending sensitive or confidential information unless it is necessary and appropriately protected.
- Not use council email accounts for personal or political campaigning purposes.

Records Management and Retention

Emails relating to council business form part of the official record. They must be filed appropriately and must be retained, archived, and disposed of in accordance with the Council's Data & Electronic Data Retention Policy.

Monitoring and Audit

The Council may audit or review council email accounts where this is necessary for legal compliance, security, or governance. Any monitoring will be proportionate and will be carried out in accordance with data protection legislation.

Reporting Security Incidents

Any suspected security incident must be reported to the Clerk immediately. This includes lost or stolen devices, lost or compromised passwords, suspected phishing or malware, and any suspected loss or unauthorised disclosure of council information.

Incidents must be reported promptly even where the person reporting believes they may be at fault. Prompt reporting allows the Council to limit the harm.

The Clerk will assess each incident and, where a personal data breach meets the statutory threshold, will report it to the Information Commissioner's Office within the required time limit.

Training and Awareness

New councillors and employees will be made aware of this policy when they take up their role.

The Council will draw users' attention to free online security training and to guidance on current risks. Users are expected to make use of it.

Breaches of this Policy

Failure to comply with this policy may result in withdrawal of access to council IT systems and accounts.

Employees

A breach may be dealt with under the Council's Disciplinary Policy.

Councillors

A breach may be referred as a complaint under the Code of Conduct.

Authorised Volunteers

The Council may withdraw authorisation to act on its behalf.

Serious breaches may be reported to the police or another appropriate authority.

Responsibilities and Contact

All users are responsible for the security of the council information and accounts they hold.

The Clerk is the point of contact for questions about this policy and for IT problems.