PINEWOOD

PARISH COUNCIL

ELECTRONIC INFORMATION AND COMMUNICATION SYSTEM POLICY 2026

Policy Statement

This policy sets out the requirements for the safe, secure and appropriate use of electronic information and communication systems used by the Parish Council and Community Hall.

The Council recognises the importance of electronic communications and digital information in delivering services, engaging with residents, managing the Community Hall, and conducting Council business. This policy aims to protect information assets, ensure compliance with legal obligations, and promote responsible use of technology.

Purpose

The Council seeks to:

- Protect electronic information from loss, damage, theft or unauthorised access.
- Ensure compliance with UK GDPR and Data Protection legislation.
- Maintain public confidence in Council operations.
- Support effective communication with residents, hall users and stakeholders.
- Reduce cyber security risks.
- Ensure business continuity.

Scope

This policy applies to:

- Parish Councillors.
- Employees.
- Volunteers.
- Contractors acting on behalf of the Council.
- Community Hall Management Committee members (where applicable).
- Any individual granted access to Council systems or information.

The policy covers:

- Computers and laptops.
- Mobile phones and tablets.
- Email systems.
- Websites.
- Social media accounts.
- Cloud-based systems.
- Electronic records and databases.
- Hall booking systems.
- Internet access.
- Digital storage devices.

Acceptable Use of Council Systems

Users must:

- Use Council systems primarily for Council business.
- Behave professionally when communicating electronically.
- Keep information secure and confidential.
- Follow all Council policies and procedures.
- Report security concerns immediately.

Users must not:

- Access inappropriate, offensive or illegal material.
- Use Council systems for personal commercial activities.
- Share passwords.

- Install unauthorised software.
- Deliberately introduce viruses or malicious software.
- Send messages that could damage the Council's reputation.

Email and Electronic Communications

Official Communications

Council business should be conducted using authorised Council email accounts wherever possible.
Users must:

- Ensure emails are accurate and professional.
- Avoid inappropriate language or comments.
- Check recipient details carefully before sending.
- Use blind copy (BCC) when sending emails to multiple external recipients where appropriate.
- Exercise caution when opening attachments or clicking links.

Email Retention

Emails that form part of Council business records shall be retained in accordance with the Council's Records Retention Policy.

Information Security

The Council will take reasonable measures to protect information, including:

- Password-protected devices.
- Multi-factor authentication (MFA) where available.
- Anti-virus and security software.
- Regular software updates.
- Secure backup arrangements.
- Restricted access to sensitive information.

Users must:

- Lock devices when unattended.
- Store confidential information securely.
- Report suspected breaches immediately.

Password Management

All users must:

- Use strong passwords.
- Keep passwords confidential.
- Change passwords if compromise is suspected.
- Use different passwords for different accounts where possible.

Passwords must never be:

- Written where unauthorised persons can view them.
- Shared with colleagues, volunteers or family members.

Data Protection and Confidentiality

The Council shall process personal data in accordance with:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Freedom of Information legislation.

Users must:

- Access only information required for their role.
- Ensure personal data is handled lawfully and securely.
- Avoid storing personal data on personal devices unless authorised.
- Report data breaches immediately to the Clerk.

Sensitive or confidential information should only be shared where there is a legitimate business need.

Use of Personal Devices
Personal devices used for Council business must:

- Be password protected.
- Have up-to-date security software.
- Be capable of secure deletion of Council information if required.

Council information must be removed when:

- A councillor or employee leaves office or employment.
- The information is no longer required.

Social Media
The Council may use social media platforms to communicate with residents and hall users.
Users authorised to manage Council social media accounts must:

- Ensure information is factual and respectful.
- Maintain political neutrality when acting on behalf of the Council.
- Protect confidential information.
- Comply with the Council's Social Media Policy.

Personal opinions must not be presented as official Council views.

Website Management
The Council's website shall:

- Publish information required by law.
- Be kept accurate and up to date.
- Include appropriate privacy notices.
- Be managed securely.

Only authorised individuals may update website content.

Community Hall Booking and Communication Systems
Where electronic booking systems are used, the Council will:

- Maintain secure access controls.
- Restrict user permissions appropriately.
- Protect customer data.
- Back up booking records regularly.

Electronic communications with hirers shall be:

- Professional.
- Consistent.
- Retained where necessary for operational purposes.

Electronic Records Management
Electronic records shall:

- Be stored securely.
- Be organised so they can be located when required.
- Be retained in accordance with Council retention schedules.
- Be disposed of securely when no longer required.

Regular backups should be undertaken to protect against data loss.

Cyber Security
The Council recognises increasing cyber security threats and will take reasonable precautions.
These may include:

- Multi-factor authentication.
- Regular password reviews.
- Security awareness training.
- Phishing awareness.
- Software updates and patching.

- Data backups.
- Incident response procedures.

Any suspected cyber incident must be reported immediately to the Clerk.

Monitoring

The Council reserves the right, where lawful and proportionate, to monitor its electronic systems to:

- Protect Council assets.
- Investigate security incidents.
- Ensure policy compliance.
- Meet legal obligations.

Users should not expect complete privacy when using Council equipment or systems for Council business

Security Incidents and Data Breaches

Any user becoming aware of:

- Loss of equipment.
- Unauthorised access.
- Malware infection.
- Accidental disclosure of information.
- Suspected phishing attacks.

must report the matter immediately to the Parish Clerk.
The Clerk will assess incidents and determine whether further reporting is required.

Training

The Council will seek to ensure that councillors, staff and relevant volunteers receive appropriate guidance and training in:

- Data protection.
- Information security.
- Cyber awareness.
- Safe use of Council systems.

Non-Compliance

Failure to comply with this policy may result in:

- Withdrawal of system access.
- Investigation by the Council.
- Disciplinary action for employees.
- Referral to relevant authorities where appropriate

Policy Review

This policy shall be reviewed every two year, unless:

- Significant technology changes;
- Following security incidents;
- Following changes to legal or regulatory requirements.

This policy was approved by the Community Hall Management Committee on 28 July 2026.

This policy was adopted by Pinewood Parish Council on 8 September 2026
Review date: September 2028