

Information Technology (IT) Acceptable Use Policy

1. Purpose

This generic policy sets out the standards for the secure, responsible and effective use of Information Technology (IT) systems and equipment owned or provided by Poulshot Parish Council.

The policy aims to:

- Protect Council information and assets.
- Ensure compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and other relevant legislation.
- Reduce the risk of cyber security incidents.
- Clarify the responsibilities of the Clerk, Responsible Financial Officer (RFO) and councillors when using Council IT systems.

2. Scope

This policy applies to:

- The Clerk to Poulshot Parish Council.
- The Responsible Financial Officer (RFO).
- Parish councillors when using Council-owned equipment, Council email accounts or accessing Council information.
- Contractors or volunteers who have been authorised to use Council IT systems.

Council IT resources include:

- Desktop computers and laptops
- Mobile phones
- Council email accounts
- Cloud storage (including Microsoft 365, OneDrive or equivalent)
- Internet access
- Website administration
- Financial software
- Printers and scanners

Poulshot Parish Council

- Any other electronic systems owned or licensed by the Council.

3. Responsibilities

The Parish Council

The Council is responsible for:

- Providing suitable and secure IT equipment where required.
- Ensuring sufficient cyber security measures are in place.
- Maintaining appropriate software licences.
- Reviewing this policy biannually.

The Clerk

The Clerk is responsible for:

- Day-to-day management of Council IT systems.
- Ensuring Council records are stored securely.
- Maintaining document filing systems and backups.
- Reporting any IT security incidents or data breaches to the Council.
- Ensuring software updates are carried out where appropriate.

The Responsible Financial Officer (RFO)

The RFO is responsible for:

- Maintaining the security of the Council's financial systems.
- Protecting electronic banking credentials and financial records.
- Ensuring financial information is securely stored and backed up.
- Verifying electronic payment requests to reduce the risk of fraud.
- Reporting any suspected financial cyber fraud immediately to the Clerk and the Council.

(Where the Clerk also serves as the Responsible Financial Officer, these responsibilities are combined.)

Parish Councillors

Councillors who access Council information electronically must:

- Keep Council information confidential.

Poulshot Parish Council

- Use Council email accounts where provided for Council business.
- Protect passwords and devices.
- Report any suspected data breaches or cyber incidents promptly.
- Comply with this policy whenever accessing Council information.

5. Monitoring

The Council may monitor the use of Council IT systems where there is a legitimate business reason, including:

- Protecting Council information.
- Investigating suspected misuse.
- Meeting legal obligations.
- Maintaining cyber security.

Monitoring will be proportionate and carried out in accordance with data protection legislation.

7. Use of Council Equipment

The Clerk and RFO are responsible for ensuring Council equipment is used primarily for Council business.

Users must:

- Lock devices when unattended.
- Keep equipment physically secure.
- Save documents in approved Council storage locations.
- Avoid storing Council documents solely on local devices.
- Report damaged or lost equipment immediately.

9. Data Protection

The Clerk and RFO are responsible for ensuring personal data is processed in accordance with the Council's Data Protection Policy.

All users must:

- Only access information necessary for their role.

Poulshot Parish Council

- Keep confidential information secure.
- Use encrypted or password-protected documents where appropriate.
- Report any actual or suspected data breach immediately.

11. Email

Council email accounts should be used for official Council business.

The Clerk and RFO should:

- Maintain professional standards in all correspondence.
- Take care when sending confidential information.
- Verify payment requests received by email before processing.
- Report phishing or suspicious emails immediately.

Councillors using Council email accounts must also comply with these requirements.

12. Internet and Social Media

Internet access is provided for Council business.

Users must not:

- Visit illegal or inappropriate websites.
- Download unauthorised software.
- Use Council systems for personal commercial activities.
- Represent the Council on social media unless authorised to do so.

14. Cyber Security and Electronic Banking

Poulshot Parish Council recognises the increasing risk of cyber crime, particularly in relation to financial transactions, email communications and the handling of personal data. The Clerk and Responsible Financial Officer (RFO) have a shared responsibility for maintaining appropriate cyber security measures.

Cyber Security

The Clerk and RFO must:

- Use strong, unique passwords for all Council systems and accounts.

Poulshot Parish Council

- Enable Multi-Factor Authentication (MFA) on Council email, banking and cloud-based systems wherever available.
- Ensure Council devices are protected with up-to-date antivirus software and operating system security updates.
- Lock devices when unattended and ensure they are stored securely.
- Be vigilant against phishing emails, fraudulent websites and other cyber threats.
- Report any suspected cyber security incident, data breach or malware infection to the Council immediately.

Councillors accessing Council systems or information electronically should also follow these security measures.

Electronic Banking

The Council uses electronic banking to manage its finances. The Clerk and RFO must ensure that all online banking is undertaken securely and in accordance with the Council's Financial Regulations.

In particular:

- Banking credentials, passwords and security devices must never be shared.
- Requests to change supplier bank details or payment instructions must always be verified independently using a trusted contact number and not solely by email.
- Any unexpected request for payment, urgent transfer of funds or changes to banking information must be treated as potentially fraudulent until verified.
- Electronic payments must only be processed following the Council's approved authorisation procedures.
- Bank reconciliations should be completed regularly and reviewed in accordance with the Council's Financial Regulations.
- Any suspected fraud, attempted fraud or unauthorised transaction must be reported immediately to the bank, the Chair of the Council and, where appropriate, the relevant authorities.

Data Backup and Recovery

The Clerk is responsible for ensuring that Council records are backed up regularly using approved storage systems. Backup copies should be tested periodically to ensure that critical information can be recovered in the event of equipment failure, cyber attack or accidental deletion.

15. Remote Working

Where Council business is conducted remotely:

- Council information must remain secure.
- Public Wi-Fi should be avoided unless a secure VPN is used.
- Confidential conversations should not take place where they may be overheard.
- Devices should never be left unattended.

16. Training

The Council will provide appropriate guidance on:

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

Users are expected to keep themselves informed of any updates to this policy.

17. Misuse of IT

Failure to comply with this policy may result in disciplinary action for employees or, in the case of councillors, referral to the Council under its adopted Code of Conduct or withdrawal of access to Council IT systems where appropriate.

Examples of misuse include:

- Sharing passwords.
- Accessing another user's account without authority.
- Installing unauthorised software.
- Using Council systems for unlawful or offensive purposes.
- Deliberately compromising Council security.
- Mishandling confidential or personal information.

18. Policy Review

Poulshot Parish Council

This policy will be reviewed biannually or sooner if required due to:

- Changes in legislation.
- New cyber security risks.
- Changes to Council IT systems.
- Recommendations from internal or external audits.

Adopted by: Poulshot Parish Council

Date Adopted: ____28th July 2026_____

Review Date: _July 2028_____

Version: 1.0