Slaley Parish Council IT Policy

1. Introduction

Slaley Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use Slaley Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Slaley Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

4. Device and software usage

Where appropriate and approved, authorised devices, software, and applications will be provided by Slaley Parish Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

All sensitive and confidential Slaley Parish Council data should be stored and transmitted securely using approved methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

(See Appendix A)

6. Network and internet usage

Slaley Parish Council's network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Slaley Parish Council are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

8. Password and account security

Slaley Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.

9. Mobile devices and remote Work

Mobile devices provided by Slaley Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

10. Email monitoring

Slaley Parish Council reserves the right to monitor email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

11. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

12. Password Security and Emergency Access – See Appendix B

Password Management - All Council IT accounts, including email, website, and cloud services, must have strong, unique passwords. Passwords must never be shared casually or stored in unsecure locations.

13. Reporting security incidents – see Appendix C

All suspected IT security breaches or incidents, including those related to email, must be reported immediately to the designated IT point of contact for investigation and resolution. The Parish Clerk and/or the Chair are the designated points of contact for all suspected or actual IT security and personal data breaches. In the absence of the Parish Clerk and/or the Chair, the Vice Chair may be contacted as an alternate point of contact.

The Clerk will liaise with the Council's website and email hosting provider for technical investigation and remediation and will assess, with appropriate advice, whether the incident requires notification to the Information Commissioner's Office.

14 Training and awareness

Where appropriate, Slaley Parish Council will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will be offered training on email security and best practices.

15. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

16. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

17. Contacts

For IT-related enquiries or assistance, users can contact Slaley Parish Council at (new email address).

All staff and councillors are responsible for the safety and security of Slaley Parish Council's IT and email systems. By adhering to this IT and Email Policy, Slaley Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Date/Minute Ref: _____

Signature: _____

Role: _____

Appendix A – Approved IT Transmissions

Appendix B – Password Security & Emergency Access

Appendix C - IT Security & Personal Data Breach Response Procedure

Approved IT Transmission Methods – Appendix A

The Parish Council will ensure that Council information and personal data are transmitted using appropriate technical and organisational measures to protect against unauthorised or unlawful processing, accidental loss, destruction, or damage.

1. **Electronic Documents**
   - Documents containing personal or sensitive information may be transmitted electronically only where:
     - Access is restricted to authorised recipients, and;
     - Files are password-protected or encrypted where the risk warrants it.
   - Passwords must be shared via a separate communication channel.

2. **Website and Hosting Services**
   - Transmission or publication of information via the Council's website must:
     - Use secure access credentials;
     - Be limited to authorised administrators;
     - Avoid publishing personal data unless there is a clear lawful basis.

3. **Cloud and Third-Party Services**
   - Only Council-approved services may be used to transmit or share information;
   - Access must be:
     - Limited to those who require it;
     - Reviewed and removed when no longer necessary.

4. **Messaging Applications (WhatsApp / Telegram)**
   - One-to-one messaging may be used for low-risk, non-confidential administrative communication only;
   - Messaging applications must not be used to transmit:
     - Personal data;
     - Confidential or sensitive information;
     - Information relating to staff matters, complaints, contracts, or finances.
   - Group messaging applications may be used only for limited, purely administrative communication;

- Permitted use includes:
  - Meeting logistics (time, venue, access arrangements);
  - Urgent practical notifications;
  - Non-confidential operational updates.
- Group messaging applications must **not** be used for:
  - Discussion, debate, or agreement of Council business;
  - Any form of decision-making or consensus-seeking;
  - Sharing personal data or confidential information;
  - Circulating documents, screenshots, or attachments.

Group messaging must not be treated as a formal communication channel. Any matter requiring a decision, record, or follow-up must be transferred to Council email or dealt with at a properly convened meeting.

Messages sent via messaging applications are not required to be retained as Council records.

5. Physical Transfer of Information

- Personal data should be transferred in physical form only where necessary
- Any removable media must be:
  - Encrypted where practicable;
  - Kept secure;
  - Safely erased or destroyed after use.

6. Incident Reporting

Any accidental or unauthorised transmission of information must be reported immediately to the Parish Clerk or Chair in accordance with the Council's IT Security and Personal Data Breach Response Procedure (Appendix C).

Password Security and Emergency Access – Appendix B

Password Management - All Council IT accounts, including email, website, and cloud services, must have strong, unique passwords. Passwords must never be shared casually or stored in unsecure locations.

Sealed Password Envelope - A physical, sealed envelope containing essential Council passwords will be maintained for emergency use only. The envelope must be:

- Clearly labelled as **"Council Emergency Passwords"**
- Stored securely in the Council office or another secure location (options are with Chair or Vice Chair
- Tamper-evident, so any breach of the envelope is immediately visible

Access to the Envelope – Access must be authorised by the Chair or Vice Chair if the Parish Clerk is unavailable. The envelope may be opened only in the event of an emergency, such as:

- The Parish Clerk is unavailable and urgent access is required
- Critical Council systems need immediate recovery or intervention

Record Keeping - Any opening of the envelope must be recorded, including:

- Date and time
- Name(s) of person(s) accessing it
- Reason for access

Passwords in the envelope must be reviewed and updated at least annually, or immediately after a breach or staff change.

IT Security & Personal Data Breach Response Procedure – Appendix C

1. Purpose

This procedure sets out how the Parish Council will respond to actual or suspected IT security incidents and personal data breaches to minimise harm, meet legal obligations, and ensure appropriate reporting.

2. Scope

This procedure applies to:

- All councillors, employees, and contractors;
- All council IT systems, including email, website, domain hosting, cloud services, and paper records containing personal data.

3. Definitions

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

An IT security breach is any incident that compromises the confidentiality, integrity, or availability of the Council's information or IT systems.

4. Reporting a Suspected Breach

Any person who becomes aware of a suspected or actual breach must:

- Report it immediately to the Parish Clerk or the Chair;
- Not attempt to investigate independently beyond securing evidence.

Examples include (but are not limited to):

- Hacked or compromised email accounts;
- Loss or unauthorised disclosure of personal data;
- Website defacement or malware;
- Emails sent to the wrong recipient containing personal data.

5. Initial Response

Upon notification, the Parish Clerk or Chair will:

- Record the incident in the Breach Log;
- Take immediate steps to contain the breach where possible;
- Contact the Council's website/email hosting provider for technical support and investigation if required.

6. Assessment

The Parish Clerk or Chair will assess:

- The type and volume of data involved;
- Whether personal data is affected;
- The potential risk to individuals (e.g. identity theft, distress, financial loss).

Advice may be sought from:

- The hosting provider;
- The Information Commissioner's Office (ICO) helpline;
- The Council's insurer or county association.

7. Reporting

If the breach is likely to result in a risk to individuals' rights or freedoms:

- The Parish Clerk or Chair will report the breach to the ICO within 72 hours;
- Affected individuals will be informed where appropriate.

All breaches, whether reported or not, will be documented.

8. Review

Following resolution, the Parish Clerk or Chair will:

- Review the cause of the breach;
- Identify any lessons learned;
- Recommend improvements to systems, training, or procedures to Council if required.