ST PAUL MALMESBURY WITHOUT PARISH COUNCIL

Information Technology (IT) and Email Policy

Introduction

St Paul Malmesbury Without 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 and employees.

Scope

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

This includes the use of personal devices to access council data, for example when councillors access council emails from their personal device.

Acceptable use of IT resources and email

The council's IT resources and email accounts are to be used for all official council-related activities and tasks. Limited personal use of council resources 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.

Device and software usage

Where possible, authorised devices, software, and applications will be provided by the council for work-related tasks. Unauthorised installation of software on authorised devices provided by the council, including personal software, is strictly prohibited due to security concerns.

Data management and security

All sensitive and confidential council data should be stored and transmitted securely using the Clerk's council devices and storage and council email accounts only. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

Regular security updates and anti-malware software are required on all council-owned and personal devices. The clerk will diary reminders to all Councillors.

Network and internet usage

This council does not currently have any network or internet connections. Should this change, any such connections should be used responsibly and efficiently for official

purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

Email communication

Council owned email accounts should be used for official business. Email accounts provided by the 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.

Password and account security

Users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong: usually this is at least 6 digits long using upper and lower case letters, numbers & special characters. Passwords should not be shared with others. Regular password changes are encouraged to enhance security.

Should any personnel or member leave the council, the Clerk (or instructed council officer or member) will rescind access to all council systems for the leaving person. This includes changing the password and freezing the email account, access to council systems (accounting software, cloud storage, website admin).

Mobile devices and remote Work

Mobile devices provided by the 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. NB, at this time, all work from home.

Email monitoring

The 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.

Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Any such archiving should be undertaken by the Clerk, rather than on Councillors' personal devices. Regularly review and delete unnecessary emails to maintain an organised inbox.

Security incidents

Definition of a Data Breach

A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- Loss or theft of devices containing personal data.
- Unauthorised access to council email accounts or files.

- Sending personal data to the wrong recipient.
- Malware or ransomware attacks compromising council systems.

Reporting a Breach

Immediate Notification: Any councillor, employee, or contractor who becomes aware of a data breach must report it immediately to the Clerk (Data Protection Officer).

Initial Response: The Clerk will assess the severity and scope of the breach and determine if mitigation steps are required (e.g., changing passwords, disabling access).

a) Investigation

A full investigation will be conducted by the Clerk or designated officer within 72 hours of the breach being discovered. The breach will be logged, including:

- Date and time of breach.
- Type and volume of data affected.
- Cause and extent of the breach.
- Actions taken to address the breach.

b) Notification Requirement

If the breach is likely to result in a risk to the rights and freedoms of individuals, the council must notify the Information Commissioner's Office (ICO) within 72 hours. If the breach poses a high risk to the individuals affected, those individuals must also be informed without undue delay, outlining:

- The nature of the breach.
- Likely consequences.
- Measures taken to mitigate the risk.
- Contact information for further support.

c) Remediation and Review

- The Clerk and council will ensure lessons are learned and policies updated.
- Procedures, or training is updated as necessary.
- Technical fixes or security upgrades will be prioritised to prevent recurrence.
- Breach logs will be reviewed periodically to identify systemic issues.

Training and awareness

The council will fund appropriate training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive training as required on email security and best practices.

Compliance and consequences

Breach of this IT and Email Policy may result in consequences as deemed appropriate.

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.

Contacts

For IT-related enquiries or assistance, users can contact the Parish Clerk in the first instance.

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

Policy adopted 27th May 2026

First review due, November 2026