



South Marston
Parish Council

IT Policy

Adopted on:	16 th December 2025
Adopted at:	Monthly Meeting Dec 2025
Last reviewed:	16 th December 2025

1. Introduction

South Marston Parish Council (SMPC) 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 SMPC's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

SMPC's 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 possible and/or necessary, authorised devices, software, and applications will be provided by SMPC 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 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.

6. Network and internet usage

SMPC does not currently provide a network or internet connectivity for any staff or councillors.

7. Email communication

Email accounts provided by SMPC are for official communication only. Emails should be professional and respectful in tone. Confidential or sensitive information must be marked as such and sent with care.

Personal email accounts should not be used to conduct council business unless there is no other option.

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

8. Password and account security

SMPC users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. Use of secure password storage lockers or similar is encouraged.

9. Mobile devices and remote Work

Mobile devices are currently not provided by SMPC.

10. Email monitoring

SMPC 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. Users should endeavour to regularly review and delete unnecessary emails to maintain an organised inbox.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately.

13 Training and awareness

SMPC will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive training on email security and best practices.

14. Compliance and consequences

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

15. 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.

16. Contacts

For IT-related enquiries or assistance, users can contact the Clerk in the first instance who may be able to offer assistance with access to council emails and files.

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