

Stoke St Mary Parish Council IT Policy

1. Introduction

Stoke St Mary 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 Stoke St Mary Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts, or prepare or handle Stoke St Mary Parish Council electronic documents using their own IT devices.

3. Acceptable use of IT resources and email

Stoke St Mary Parish Council (SSM PC) 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, authorised devices, software, and applications will be provided by Stoke St Mary Parish Council for work-related tasks; however, resource constraints preclude the provision of SSMPC owned devices for all officers. Councillors, volunteers, employees and contractors are therefore authorised to use their own devices for SSMPC business, subject to adoption of the data management and security provisions below.

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

5. Data management and security

When creating or managing general SSMPC documents or data, whether on an SSMPC or on a personal device, conventional security protections should be used,

as you would do if managing your own information prudently. These include password or biometric protections for device access, ensuring that operating software protections such as Windows Security are enabled, or replaced by a licensed security package such as McAfee. All sensitive and confidential Stoke St Mary Parish Council documents / data should be stored and transmitted securely, including the use of document passwords / encryption when being transmitted. Cloud or regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when deleting SSMPC data. Any device that has been used for SSMPC business should have SSMPC data, documents and software removed before disposal or transfer.

6. Network and internet usage

Stoke St Mary 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 Stoke St Mary 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

Stoke St Mary 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

Devices provided by Stoke St Mary Parish Council should be secured with passcodes and/or biometric authentication for access.

10. Email monitoring

Stoke St Mary 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. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

13 Training and awareness

Stoke St Mary Parish Council will provide appropriate training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive appropriate training / guidance 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 Clerk-
clerk@stokestmaryparish.gov.uk

All staff and councillors are responsible for the safety and security of Stoke St Mary Parish Council's IT and email systems. By adhering to this IT and Email Policy, Stoke

St Mary Parish Council aims to create an appropriately secure and efficient IT environment that supports its mission and goals.

Date: 16th July 2026

Signature: Sarah Fisher

Role: Clerk