

Sturton by Stow Parish Council

IT Policy

1. Introduction

Sturton by Stow 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 Sturton by Stow parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Sturton by Stow 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 possible, authorised devices, software, and applications will be provided by Sturton by Stow 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 Sturton by Stow 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.

6. Network and internet usage

Sturton by Stow 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. The use of Artificial Intelligence (AI)

Councillors recognised that AI can be a useful tool for assisting with administrative tasks such as drafting documents and improving written communications. However, it is understood that AI should be used responsibly and with appropriate safeguards.

Confidential, personal or sensitive information must not be entered into AI systems. This includes information that could identify the Parish Council, its location, individual councillors, members of staff, residents, or any other data that is not already in the public domain. Any information or documents produced using AI must be carefully reviewed and verified by the Clerk or an appropriate officer before being relied upon or published, as AI-generated content may contain inaccuracies or outdated information.

8. Email communication

Gov.uk Councillor email accounts provided by Sturton by Stow 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.

9. Password and account security

Sturton by Stow parish council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and only shared with the Clerk. Regular password changes are encouraged to enhance security; Councillors are reminded to always keep the Clerk up to date with password changes.

10. Mobile devices and remote Work

Mobile devices provided by Sturton by Stow 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.

11. Email monitoring

Sturton by Stow 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.

12. 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.

13. 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.

14 Training and awareness

Training can be accessed through LALC to educate users about IT security best practices, privacy concerns, technology updates and email security.

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 The Clerk

E-mail: clerk@sturtonbystow-pc.gov.uk

Phone:07476902278

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

This Policy was adopted by Sturton by Stow Parish Council: July 2025

Reviewed: July 2026- Introduction of Section 8. The use of AI, change in councillor emails to gov.uk Accounts and recommendation to have councillors sign a hard copy of the IT Policy to show compliance.

Date of Next Review: July 2027

Declaration

I confirm that I will abide by this policy:

_____ Chairman

_____ Vice Chairman

_____ Councillor

_____ Councillor

_____ Councillor

_____ Councillor

_____ Clerk