St Helen Without Parish Council
Working for You

Approved by the Council on 23rd June 2025

St Helen Without Parish Council IT Policy

1. Introduction

St Helen 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, employees, volunteers, and contractors.

2. Scope

This policy applies to all individuals who use St Helen Without Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

St Helen Without Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. 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 St Helen Without 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 St Helen Without 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

If provided, St Helen Without 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 St Helen Without 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

St Helen Without 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 St Helen Without 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

St Helen Without 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

Email accounts should be regularly reviewed and unnecessary emails be deleted to maintain an organised inbox and to avoid excessive storage being required.

Emails should be retained until the information contained has been resolved or superseded such for example as emails recording policy decisions, delegated authorities, legal advice, or committee instructions; once these decisions have been recorded in the minutes of the next appropriate meeting, the emails should then be deleted.

Where information contained within an email is required for longer term reference, users should consider saving these to file storage as PDF documents within the Council's Cloud storage to make the content available to other members of the Council. Examples:

- Finance – orders, invoices
- Contracts - tender invitations, clarifications, contract negotiations
- Complaints, FOI, Subject Access Requests - investigations, and outcomes

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

St Helen Without Parish Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will receive appropriate 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.

All staff and councillors are responsible for the safety and security of St Helen Without Parish Council's IT and email systems. By adhering to this IT and Email Policy, St Helen Without Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.