SPEEN PARISH COUNCIL

Speen Parish Council

IT and Email Policy

1. Introduction

Speen 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.

All members of staff and councillors are responsible for the safety and security of Speen Parish Council's IT and email systems. By adhering to this IT and email policy Speen Parish Council aim to create a secure and efficient IT environment.

2. Scope

2.1 The policy applies to all individuals who use Speen Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

2.2 This policy should be read in conjunction with Speen Parish Council's Risk Management Policy, Data Protection Policy, Freedom of Information Policy and the Councillor's Code of Conduct.

3. Acceptable use of IT resources and email accounts

Speen Parish Council's IT resources and email accounts are to be used for official council-related activities and tasks only. 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

4.1 Where possible authorised devices, and applications will be provided by Speen Parish Council for work related tasks.

4.2 Unauthorised installation of software on authorised devices, including personal software is strictly prohibited due to security concerns.

5. Data Management and Data Security

All sensitive and confidential Speen 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, in accordance with Speen Parish Council's Data Protection and Document Retention Policies.

6. Network and Internet Usage

Speen 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.

FINAL

7. Email communication

7.1 Email accounts provided by Speen Parish Council are for official communications only. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

7.2 You must not download any attachments or click any links before verifying the source.

7.3 Use of any other email addresses is **actively discouraged** by the Council and will be at the individual's personal risk, including following Data Protection principles.

7.4 Speen Parish Council accepts no liability whatsoever for any loss or damage caused through use of personal email addresses and any other third-party IT systems used for Speen Parish Council business.

7.5 Speen Parish Council must have access to all its records, including emails, in order to carry out its business and to meet its obligations for accountability and transparency. Emails, therefore, need to be managed as any other Council record in accordance with the law and this policy.

7.6 Emails belong to the Council and form part of the Council's records and must be readily retrievable by the Clerk. This data may need to be retrieved at relatively short notice, and all councillors will be expected to allow the Clerk access to Council email addresses following a written Freedom of Information request, as required, in order to perform their duties in these circumstances.

7.7 Emails sent or received while on Council business are the property of the Council and must not be considered as the personal property of the sender or receiver.

7.8 Members and staff are individually and equally responsible for ensuring appropriate use of email, including, following Data Protection principles

7.9 Speen Parish Council members recognise that all emails relating to Speen Parush Council business, whether those issued by the council, or where a Councillor uses personal / workplace email addresses against the advice of the Council and this policy, will be subject to the Freedom of Information Act 2000 and as such may be searched and used as evidence in event of an FOI investigation.

8. Email Etiquette

8.1 Email use is an enhancement to decision-making and recording of process, not a substitute. All decision-making should be made through normal council procedures i.e. Council meetings wherever possible.

8.2 The use of email to exchange correspondence requires councillors and staff to conform to the same level of scrutiny as all other means of communication. It is expected that operators will respect the same professional standards in email as in other forms of communication i.e. follow the Speen Parish Council Code of Conduct and such procedural and legal constraints as apply to all other activities.

8.3 You should not send or forward mail which is defamatory or offensive under any circumstances.

8.4 Agreements made by email are most likely to have the same status as letters or formal contracts. Therefore, you should be circumspect in use of emails for such correspondence.

8.5 You must not include in the text of emails to be sent, or in files attached to them, sensitive personal data without appropriate protection in order to comply with GDPR. (Refer

to Speen Parish Council Data Protection Policy for further information about what constitutes sensitive data).

8.6 Email addresses should be treated as confidential, and adequate care taken that private email addresses are not openly circulated. Email to multiple addresses outside of Councillors and the Clerk should be sent as blind copy (bcc).

8.7 The following activities are prohibited from SPC email addresses and equipment:

- **Disrepute:** Any activity which might damage the reputation of the Council, its employees or members.
- **Spamming and Invasion of Privacy:** Sending of unsolicited bulk and/or commercial messages or activities that invade another's privacy
- **Intellectual Property Right Violations:** Engaging in any activity that infringes or misappropriates the intellectual property rights of others, including patents, copyrights, trademarks, service marks, trade secrets, or any other proprietary right of any third party.
- **Obscene or Indecent Speech or Materials:** to advertise, solicit, transmit, store, post, display, or otherwise make available obscene or indecent images or other materials. SPC will notify and fully cooperate with the police and any law enforcement agency if it becomes aware of any use of the service in any connection with such activities.
- **Defamatory or Abusive Language:** Using the service to transmit, post, upload, or otherwise making available defamatory, harassing, abusive, or threatening material or language that encourages bodily harm, destruction of property or harasses another.
- **Hacking:** Accessing illegally or without authorisation computers, accounts, equipment or networks belonging to another party, or attempting to penetrate security measures of another system. This includes any activity that may be used as a precursor to an attempted system penetration, including, but not limited to, port scans, stealth scans, or other information gathering activity.
- **Distribution of Internet Viruses,** Trojan Horses, or Other Destructive Activities: Distributing information regarding the creation of and sending Internet viruses, worms, Trojan Horses, pinging, flooding, etc
- **Other Illegal Activities:** violation of applicable law and regulation, including, but not limited to, advertising, transmitting, or otherwise making available pyramid schemes, fraudulently charging credit cards, pirating software, or making fraudulent offers to sell or buy products, items, or services.

9. Password and account security

Speen Parish Council users are responsible for maintaining the security of their accounts and passwords. Passwords should be strong and not shared with others. The Clerk must retain access to all email inboxes at all times. Councillor passwords will be set by the Clerk and must not be changed.

10. Mobile devices and remote working

Mobile devices provided by Speen 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 an office.

11. Email monitoring

Speen 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

12.1 Emails should be retained and archived in accordance with the Council's Document Retention Policy and in accordance with any legal and regulatory requirements.

12.2 Staff and members should regularly review and delete unnecessary emails to maintain an organised inbox.

13. Reporting Security Incidents

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

14. Training

Staff and members may access training in the use of new technology if deemed necessary.

15. Compliance and consequences

Any breaches in this IT and email policy will be investigated and any action arising will follow the council's disciplinary procedures.

16. Policy review

This policy will be reviewed every three years to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

17. Contacts

For any queries with reference to this policy, please contact the Clerk.

18. Authorisation

This policy has been authorised by Speen Parish Council as follows:

Adopted by The Council on:	8th October 2025
Last Review:	14th October 2026
Next Review	14th October 2029

FINAL