ST BRIAVELS PARISH COUNCIL

IT & EMAIL POLICY

Adopted **Feb 2026**

Reviewed **NEW**

Next review **Feb 2028** or earlier if required

St Briavels Parish Council

IT & Email Policy

1. Introduction

St Briavels 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, (includes temporary staff, volunteers and contractors granted approved access).

2. Scope

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

Use of own device and email requirements are also included for Councillors to aim to minimise security risk as far as possible or practical.

3. Acceptable use of IT resources and email

St Briavels 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. Council Device and software usage

Where possible, authorised devices, software, and applications will be provided by St Briavels 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 Briavels 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

St Briavels 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.

Staff and Councillors must ensure only secure WiFi networks are used. If transferring data, either by email or by other means, this should be done through an encrypted

channel, such as a virtual private network (VPN) or a secure web protocol (https://). Unsecured wireless networks should not be used on council or personal devices.

7. Email communication

Email accounts provided by St Briavels 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.

Particular caution must be observed regarding email attachments and links to avoid phishing and malware. Ensure senders are genuine and verify the source before opening any attachments or clicking on links. Delete suspicious emails.

All St Briavels Parish Council business emails should be actioned from the Clerk on behalf of the Council. Councillors' council business emails must copy in the Clerk to ensure the Clerks official account records and appropriately holds all council business.

8. Password and account security

St Briavels 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.

Users accessing council IT systems such as email and messaging services should ensure that the devices used are protected by a secure password (ideally biometric authentication) and have an active mechanism in place to protect against viruses, phishing and malware.

9. Mobile devices and remote Work

Mobile devices provided by St Briavels Parish Council should be secured with appropriate strong passcodes (ideally biometric authentication). When working remotely, users should follow the same security practices as if they were in the office.

Mobile devices must be stored safely and securely when not in use in the office or working from home. When travelling equipment should not be left unattended and never be left in parked vehicles or at any council or non-council premises.

St Briavels Parish Council is only a small organisation therefore allowing use of personal devices and email accounts by Councillors is unavoidable. The Information Commissions "Bring Your Own Device" guidance must be followed by Councillors when using personal devices for council business, along with this policy as appropriate to minimise and mitigate security risks as far as possible and practical.

Councillors must take responsibility for understanding how their devices may compromise St Briavels Parish Council if data is misused or inappropriately stored or retained. Appropriate training and support will be given.

10. Email monitoring

St Briavels Parish Council reserves the right to monitor its email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

Unless provided by St Briavels Parish Council, Councillors must have an approved specific email account for use explicitly for council business only Access must be appropriately secure and never shared. In very extreme cases of serious legal proceedings against the council, it's possible a device, whether council-owned or personal, may be temporarily taken to view emails or retrieve the relevant data.

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. This applies to council owned and councillors designated email accounts on personal devices.

12. Reporting security incidents

All suspected security breaches or incidents including email-related should be reported immediately for investigation and resolution. For St Briavels Parish Council contact the Clerk (or Responsible Officer).

13 Training and awareness

St Briavels 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 regular training on email security and best practices.

14. Compliance and consequences

Breach of this IT & Email Policy may result in the suspension of IT privileges and further consequences as deemed appropriate for the misuse and possible misconduct.

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 or email related enquiries, contact the Clerk or Responsible Officer.

All staff and councillors are responsible for the safety and security of St Briavels Parish Council's IT and email systems. By adhering to this IT and Email Policy, St Briavels Parish Council aims to create a secure and efficient IT environment that supports its mission and goals, follows good practice and complies with its legal and professional obligations.

Note: The SAPP template for parish councils has been copied and appropriately customised for this small council (EH Jan 2026).