



IT and Email Policy

1. Introduction

Buriton 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 guidelines and responsibilities for the appropriate use of IT resources and email by councillors, employees, volunteers and contractors.

2. Scope

This policy applies to all councillors and employees.

3. Acceptable use of IT resources and email

Buriton Parish Council's 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. Devices and Software usage

Where possible, authorised devices, software and applications will be provided by Buriton 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 Buriton Parish Council's data should be stored and transmitted securely using appropriate methods. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

6. Internet usage

Buriton Parish Council's 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 Buriton 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.



BURITON PARISH COUNCIL

8. Password and account security

Buriton Parish Council councillors and employees 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

Mobile devices provided by Buriton Parish Council should be secured with passcodes and/or biometric authentication.

10. Email monitoring

Buriton 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 Clerk and Chair for investigation and resolution. Report any email-related security incidents or breaches to the Clerk and Chair immediately.

13. Training and awareness

Training and resources to educate users about IT security best practices, privacy concerns, and technology updates will be provided.

14. Compliance and consequences

Breach of this IT and email policy may result in suspension of IT privileges and other consequences as deemed appropriate.

15. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be to address emerging technological trends and security measures.

16. Contacts

For IT-related enquiries or assistance, councillors and employees can contact the Clerk.

All councillors and employees are responsible for the safety and security of Buriton Parish Council's IT and email systems. By adhering to this IT and Email Policy, Buriton Parish Council aims to create a secure and efficient IT environment that supports its' missions and goals.