Allington Parish Council IT Policy

1. Introduction

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

3. Acceptable use of IT resources and email

Allington 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 Allington 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 Allington 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

Allington parish council does not provide network and internet connections directly but users should ensure that any networks and internet connections they do use

are secure using password protection and parish council communications are not being intercepted. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Email communication

Email accounts provided by Allington 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

Allington 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 are not provided by Allington parish council so users will be using their own equipment and that equipment should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were working in an office environment.

10. Email monitoring

Allington 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, GDPR and the Freedom of Information Act.

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 for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately. The Clerk has delegated authority to deal

with providers of the council's IT products and services and to obtain professional IT support to secure equipment, email accounts and data and fix faults and deal with breaches and incidents in accordance with advice and guidance of the Information Commissioners Office (and its successors), the council's Financial Regulations and Standing Orders.

13 Training and awareness

Allington 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 either regular training or awareness updates 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 bi-annually to ensure its relevance and effectiveness or earlier when 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 to Allington Parish Council.

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

This policy was adopted by Allington Parish Council in Minute 35/26 on 18/03/26.

FOR REVIEW MAY 2027