Winsley Parish Council

IT POLICY

1. Introduction

Winsley 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 councillors, the Clerk, volunteers, and contractors. The purpose of this policy is to ensure that all Parish Council business is conducted securely, legally and in line with best practice, including the Practitioner's Guide and the National Association of Local Councils (NALC) guidance.

2. Scope

This policy applies to all individuals using IT, software or email for Parish Council work, whether on council-owned or personal devices.

3. Device and software usage

Personal devices may be used for parish council work if secure, updated, and password-protected. Winsley Parish Council will keep the possible provision of authorised devices, software, and applications for work-related tasks under review.

4. Acceptable use of IT resources and email

Any individual using Winsley Parish Council IT resources and email accounts for official council-related activities and tasks must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy.

5. Data management and security

All sensitive and confidential 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.

Downloading and sharing copyrighted material without proper authorisation is prohibited.

6. Email communication

Email accounts provided by Winsley 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.

DRAFT

Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

7. Password and account security

When working on Winsley Parish Council business, individuals 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.

8. Email monitoring

Winsley 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.

9. 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.

10. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk for investigation and resolution. The Clerk will assess if notification to the Information Commissioner's Office (ICO) is required within 72 hours.

11. Training and awareness

The Clerk and Councillors will receive training and resources to educate users about IT and email security best practices, privacy concerns, and technology updates.

12. 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.

13. Contacts

For IT-related matters contact the Clerk: parishclerk@winsley.org.uk.

DRAFT