WILLAND PARISH COUNCIL

IT POLICY

1. Introduction

Willand 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 Willand Parish Council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

The 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. Device and software usage

Where possible, authorised devices, software, and applications will be provided by the Council for work-related tasks.

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

Councillors are not provided with Council authorised devices and must ensure that all software and applications used on personal devices for Council business are appropriately secured and kept private to minimise the potential for unauthorised access.

5. Data management and security

All sensitive and confidential Willand Parish Council data will be stored and transmitted securely using approved methods. Regular data backups will be performed to prevent data loss, and secure data destruction methods will be used when necessary.

The Council stores its electronic data and records in a secure, password protected cloud with access to documentation and information restricted to those who require it for the performance of their duties.

The Council's General Data Protection Regulations – Privacy Policy sets out how information is collected, used and stored.

6. Network and internet usage

The Council does not have an office or other buildings and has no network and internet connections other than separate password protected Wi-Fi access at the village hall, which should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material over this connection or when using Council resources without proper authorisation is prohibited.

7. Email communication

The Council provides staff and councillors with Parish Council .gov email accounts. These are for official communication only. Emails should be professional and respectful in tone. Care must be taken when sending confidential or sensitive information to ensure it is sent securely and only to those entitled to the information. The Council's General Data Protection Regulations – Privacy Policy sets out how information is used and shared.

Be cautious with attachments and links in emails to avoid phishing and malware. Verify the source before opening any attachments or clicking on links. Emails, attachments or links must not be opened if the recipient has any suspicion that they are not genuine or may cause a security issue.

8. Password and account security

All 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 provided by the Council should be secured with passcodes and/or biometric authentication. When accessing Council emails and information remotely users should follow the same security practices as if they were in an office.

Councillors are not provided with Council authorised mobile devices and must ensure that all software and applications used for Council business are appropriately secured and kept private to minimise the potential for unauthorised access.

10. Email monitoring

The 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 Parish Clerk for investigation and resolution.

13 Training and awareness

The Council will provide regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All staff and councillors will receive regular training and updates on email security and best practices.

14. Compliance and consequences

Breach of this Policy may result in the suspension of IT privileges and further consequences as deemed appropriate.

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-related enquiries or assistance, users should contact the Parish Clerk.

All staff and councillors are responsible for the safety and security of the Council's IT and email systems.

This policy was approved and adopted by Willand Parish Council on the 12th June 2025