

Willington Parish Council IT (Information Technology) Policy

1. Introduction

Willington Parish Council recognises the importance of effective and secure information technology (IT) and email 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, employees, volunteers and contractors.

2. Scope

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

3. Acceptable use of IT resources and email

Willington Parish Council's IT resources and email accounts are to be used for official council-related activities and tasks. No personal use is permitted. All users must adhere to ethical standards, respect copyright and intellectual property rights, and must not access inappropriate or offensive content.

4. Device and software usage

Authorised devices (a laptop and a printer), software and applications will be provided by Willington Parish Council to the Clerk for work-related tasks. Unauthorised installation of software on these authorised devices is strictly prohibited.

Councillors will access their Parish Council e-mail account and related documents e.g. meeting papers on Google share, from their own mobile, tablet and desktop/laptop devices. Councillors must take reasonable steps to secure their personal devices for example ensure that anti-virus software is installed on their devices and is up to date. Councillors must, as a minimum, password protect their device and keep it physically secure.

5. Data management and security

All sensitive and confidential Willington Parish Council data should be stored and transmitted securely using approved methods such as password protected files or encryption. Regular data backups shall be performed to prevent data loss e.g. via Microsoft OneDrive sync and backup. Secure data destruction methods shall be used when necessary.

6. Network and internet usage

Internet access from the Willington Parish Council's laptop should be used responsibly and appropriately for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited. Willington Parish Council does not have an IT network.

7. Email communication

Email accounts provided by Willington Parish Council are for official communication only. They shall be used for all Parish Council related e-mail, to ensure Council Members and the Clerk comply with UK GDPR. The e-mail domain is willingtonparish.gov.uk.

Councillor email accounts will be: firstname.surname@willingtonparish.gov.uk. The Clerk's email account will be: clerk@willingtonparish.gov.uk

All emails shall be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

8. Password and account security

Willington 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

The laptop provided by Willington Parish Council for use by the Clerk shall be secured with passcodes and/or biometric authentication. All applications used by the Clerk on the laptop e.g. Sage payroll software should have a unique user id and a strong password. Two factor authentication should be used if appropriate and available.

The Clerk shall ensure anti-virus software is installed and up to date on the laptop, e.g. Microsoft Defender Antivirus, which is built into Windows 10 and 11 and provides real-time protection against malware and other threats. The laptop shall be kept physically secure.

10. Email monitoring

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

11. Retention and archiving

Emails should be retained and archived in accordance with business requirements, and legal and regulatory requirements. Email folders should be regularly reviewed and unnecessary emails deleted to maintain an organised Inbox, and adhere to UK GDPR and Data Protection Act laws.

Other Parish Council owned data e.g. mailing lists and the PC website must be regularly audited by the Clerk in line with UK GDPR and the Data Protection Act. Remedial actions e.g. deletion of outdated personal data will then be completed to maintain compliance.

12. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk and Chairman for investigation and resolution.

13 Training and awareness

Willington Parish Council will provide training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and Councillors will receive training on IT and email security and best practices.

14. Compliance and consequences

Breach of this IT 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, revised legislation and security measures.

16. Contacts

For IT-related enquiries or assistance, users should initially contact the Clerk.

All staff and Councillors are responsible for the safety and security of Willington Parish Council's IT and email systems. By adhering to this IT Policy, Willington Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

Policy adopted by Willington Parish Council

Date: 25th November 2025

Minute: 25/098

Next Review Date: November 2026