WHPC
West Hill Parish Council

West Hill Parish Council
IT Policy

APPROVED at WHPC Meeting 2nd September 2025 Min 25/293

1. Purpose and Scope

The purpose of this policy is to establish the guidelines, responsibilities and standards for the use of IT equipment and systems provided and used by West Hill Parish Council (WHPC).

This policy applies to all individuals including Councillors, employees and volunteers who use WHPC's IT resources, including computers, software, devices, data, and email accounts.

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

This policy should be read in conjunction with the linked policies listed below:

- Code of Conduct
- Data Protection Policy
- Communications Policy (Social Media)
- Data Breach Policy

2. Policy Statement

IT equipment and systems provide a means of communication and data storage and handling which can contribute to the efficient and effective conduct of the Council.

The widespread use of IT systems and social media applications has resulted in laws and regulations governing the use of such systems. All data stored and handled on WHPC equipment and systems must be carefully protected. All users of IT equipment and systems working for and on behalf of WHPC must:-

- Comply with all laws concerning the use of IT systems including Data Protection, Health and Safety, Equality and all other related matters
- Not use the equipment or systems in any way that may harm the reputation of WHPC.
- Adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.
- Treat all WHPC supplied equipment with care to protect against loss or damage
- Use WHPC equipment only for Council related business and not for personal use.
- Not use personal IT equipment (such as mobile phones) for storage or processing WHPC data or for other WHPC business without specific authorisation from the Parish Clerk

The Parish Council is both the Data Controller and a Data Processor.

3. User Accounts

WHPC must have-an authority owned domain.

WHPC Users will also have e-mail accounts hosted on the same domain. All WHPC user accounts will be created by the Parish Clerk.

4. Device and Software Usage

IT equipment refers, but Is not limited to computer, internet access, phones owned by the Council.

Where possible, authorised devices, software, and applications will be provided by WHPC for Parish Council business.

Mobile devices provided by WHPC must be secured with passcodes and/or biometric authentication. As most users will be working remotely, users must pay particular attention to adhering strictly to security measures and practices.

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

Use of WHPC provided equipment for personal purposes is not permitted without specific approval from the Parish Clerk.

5. Internet Usage

WHPC's internet connections must be used responsibly and efficiently and only for official WHPC purposes.

Downloading and sharing copyrighted material without proper authorisation is prohibited. Be cautious with attachments and links to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

6. Email Communication

Email accounts provided by WHPC are for official communication only. Emails must be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.

All official WHPC communications must only be sent from a council-owned email address

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

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox.

WHPC 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.

7. Data Management and Security

All sensitive and confidential WHPC data must be stored and transmitted securely using approved methods. Regular data backups must be performed to prevent data loss, and secure data destruction methods should be used when necessary.

Personal data must not be stored unencrypted on USB sticks, personal laptops, or cloud services unless approved by the council.

8. Password and Account Security

WHPC 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. Website

The WHPC website must meet the standard of the latest approved Web Content Accessibility Guidelines and the Public Sector Bodies (Websites and Mobile Applications)(No.2) Accessibility Regulations 2018. The website must include published documentation as specified in the Freedom of Information Act 2000 and the Transparency Code for smaller authorities.

10. Social Media

Accessing social media using WHPC provided devices or using social media for WHPC business must only be done with explicit authority from the Parish Clerk and may require the user to undergo training. When posting information on social media it must be remembered that this may become widely available and may be taken to reflect WHPC's official position on the matter concerned.

The following guidelines must be followed when using social media on behalf of WHPC:-

- No information that is considered to be confidential is to be posted on any social media platform.
- No defamatory or disparaging statements or comments may be posted on any social media platforms.
- Any comments that may be seen as speaking on behalf of WHPC must be approved beforehand by the Parish Clerk and Chairman.
- Any content seen on social media that disparages or reflects poorly on WHPC must be reported immediately to the Parish Clerk who will arrange for a response to such comments if it is deemed necessary.

11. Reporting Security Incidents

Any suspected security breaches or incidents must be reported immediately to the Parish Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Parish Clerk immediately.

12. Training and Awareness

WHPC 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 regular training on email security and best practices.

13. Policy Review

This policy will be reviewed at least annually to ensure its relevance and effectiveness. Updates may be made from time to time to address emerging technology trends and security measures.

14. Declaration

Annually, Councillors will be asked to declare they have read, understood, and accepted the conditions of the West Hill Parish Council IT Policy.(Appendix 1)

This policy should be reviewed annually. Next review May 2026.

Appendix 1

West Hill Parish Council
IT Policy
Councillor Declaration

Declaration

This declaration should be signed by the Councillor upon joining the Council, and/or annually thereafter.

I confirm that I have read, understood, and accept the conditions of the West Hill Parish Council IT Policy.

Councillor Name: ____________________________________

Councillor Signature: ____________________________________

Date: ____________

Witnessed By:

Parish Clerk: ____________________________________

Officer Signature: ____________________________________

Date: ____________