Therfield Parish Council

IT Policy

Based upon the Smaller Authorities' Proper Practices Panel (SAPPP) 2025

1. Introduction

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

3. Acceptable use of IT resources and email

Therfield Parish 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 Therfield Parish Council for work-related tasks.

Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns. Council laptops must not have software installed without prior consent.

5. Data management and security

All sensitive and confidential Therfield 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.

The Therfield Parish Council acts as Data Controller under GDPR legislation. No personal data should be stored unencrypted on personal devices or cloud platforms without council approval.

6. Network and internet usage

Therfield Parish Council ’s network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

7. Cybersecurity Best Practices

The Therfield Parish Council require anti-virus protection and regular updates. Only the Clerk is authorised to post on the council’s official social media pages if relevant.

8. Email communication

Email accounts provided by Therfield 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.

The Therfield Parish Council require the use of an official, generic council email (name@therfieldparishcouncil.gov.uk) for all correspondence on the council’s own domain

9. Password and account security

Therfield 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.

10. Mobile devices and remote Work

Mobile devices provided by Therfield Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

11. Website and Accessibility Standards

The Therfield Parish Council will ensure the council website complies with WCAG 2.2 AA standards and publishes required content (for example minutes, AGAR, councillor information)

12. Email monitoring

Therfield 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.

13. 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.

14. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the designated IT point of contact for investigation and resolution. Report any email-related security incidents or breaches to the IT administrator immediately.

15. Training and awareness

Therfield 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 regular training on email security and best practices.

16. Compliance and consequences

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

17. 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.

18. Contacts

For IT-related enquiries or assistance, users can contact the Therfield Parish Council Clerk

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

Date Adopted: 11th November 2025

Minute Reference: 10.11.25

Review Date and Minute:	
Review Date and Minute:	
Review Date and Minute:	