Heighington Parish Council

IT Policy

Document Ref:	POL/IT
Status:	Approved
Version:	2.0
Date of approval:	10/02/25
Minute reference:	206/M/24
Date of next review:	February 2027

Version Control:

Version: 2.0
Amended by: Clerk
Date approved: 10/02/25
Amendments: Government model template adopted, replacing ICT Policy.
Minute reference: 206/M/24

Version: 1.0 (ICT Policy)
Document creation by: Clerk
Date approved: 14/03/22
Minute reference: 184/M/21

1. Introduction and purpose

1.1 Heighington parish council ("the parish council") recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.

1.2 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

2.1 This policy applies to all individuals who use the parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

3 Acceptable use of IT resources and email

3.1 The parish council 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.

3.2 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

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

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

5 Data management and security

5.1 All sensitive and confidential parish council data should be stored and transmitted securely using approved methods.

5.2 Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

6 Network and internet usage

6.1 The 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 Email communication

7.1 Email accounts provided by the 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.

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

8 Password and account security

8.1 The 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

9.1 Mobile devices provided by the 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.

10 Email monitoring

10.1 The 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.

11 Retention and archiving

11.1 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

12.1 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.

13 Training and awareness

13.1 The 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.

14 Compliance and consequences

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

15 Policy review

15.1 This policy will be reviewed bi-annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

16 Contacts

16.1 For IT-related enquiries or assistance, users can contact the clerk.

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

I confirm that I will abide with this Policy:

Date: _____

Signature: _____

Role: _____