



ITC POLICY

1. Introduction

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

3. Acceptable use of IT resources and email

Nassington 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. 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 Nassington Parish Council for work-related tasks.

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

5. Data management and security

All sensitive and confidential Nassington 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.

6. Network and internet usage

Nassington 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

Email accounts provided by Nassington 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.

8. Password and account security

Nassington 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

Mobile devices provided by Nassington Parish Council 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

Nassington 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

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

13. Bring Your Own Device (BYOD)

The Council recognises that councillors and the clerk may use their personal devices (such as laptops, tablets, and mobile phones) to access council information. To protect council data and reduce risk, the following expectations apply:

i. Use of Personal Devices

- Personal devices may be used for council business where convenient.
- Users are responsible for keeping their own devices in good working order and ensuring they have reliable internet access.

ii. Security Measures

- Devices used for council business must be protected by a passcode, password, fingerprint or equivalent lock.
- Antivirus or built-in security updates must be kept current, and automatic updates enabled where possible.
- Where a device is shared with other household members, the councillor or clerk must use a separate user account/login that only they can access. Council information must not be accessible from any shared or guest account.
- Confidential documents stored in cloud storage must be secured with two-factor authentication and in a manner compliant with prevalent GDPR / Data Protection regulations

iii. Data Handling

- Council documents should be stored within approved platforms (e.g., council email accounts, cloud storage managed by the council) and not permanently downloaded or saved to personal hard drives unless necessary for immediate work.
- Council data must not be shared, copied, or stored in a way that risks unauthorised access.

iv. Loss or Theft

- Any loss, theft or compromise of a device used for council business must be reported to the clerk as soon as possible so that passwords can be changed and risks managed.

v. Privacy

- The council will not access the personal content of any individual's device.
- However, users must cooperate if data relevant to council business is required under Freedom of Information, Subject Access Requests, audit or legal process.

vi. End of Role or Change of Devices

- When a councillor leaves office or a device is replaced, all council data must be deleted from the old device.

14. Training and awareness

Nassington Parish Council will facilitate regular training and resources to educate users about IT security best practices, privacy concerns, and technology updates. All employees and councillors will have access to training on email security and best practices.

15. Compliance and consequences

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

16. 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.

17. Contacts

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

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

18. Adoption and Review

This policy was adopted at the Deember 2025 meeting of Nassington Parish Council and will be reviewed annually at the council's annual parish council meeting in May or sooner if required by legislation or local circumstances.

19. Contact Details

Parish Clerk

Email: clerk@nassington-pc.gov.uk

Address: PO Box 1610, PETERBOROUGH, PE2 2BB

Phone: 01780 435084 / 07352 063726

Chair of the Council

Email: chair@nassington-pc.gov.uk