



IT POLICY

The IT Policy was first adopted by the Council at its meeting held on 23rd April 2026. It will be reviewed annually or in the event of major legislative change.

	Date	Minute Reference
Adopted	23/04/2026	25/470
Next Review	April 2027	

Contents	Page
1. Introduction	3
2. Scope	3
3. Acceptable use of IT resources and email	3
4. Device and software usage	3
5. Data management and security	3
6. Network and internet usage	3
7. Email communication	3
8. Password and account security	4
9. Mobile devices and remote work	4
10. Email monitoring	4
11. Retention and archiving	4
12. Reporting security incidents	4
13. Training and awareness	4
14. Compliance and consequences	4
15. Policy review	4
16. Contacts	4

1. Introduction

- 1.1 Nazeing 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 Nazeing Parish Council IT resources, including computers, networks, software, devices, data and email accounts.

3. Acceptable Use of IT resources and email

- 3.1 Nazeing 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

- 4.1 Where possible, authorised devices, software, and applications will be provided by Nazeing Parish Council for work-related tasks. However, it is also recognised that as a small parish council with limited resources this may not always be possible and it is the likelihood that personal devices will be used.
- 4.2 Unauthorised installation of software on council-owned devices, including personal software, is strictly prohibited due to security concerns.

5. Data management and security

- 5.1 All sensitive and confidential Nazeing 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

- 6.1 Nazeing Parish Council network and internet connections should be used responsibly and efficiently for official purposes. Downloading and sharing copyrighted and confidential material without proper authorisation is prohibited.

7. Email communication

- 7.1 Email accounts provided by Nazeing Parish Council are for official use only and must always be used for any Council related communications. Emails should be professional and respectful in tone. Confidential or sensitive information must not be sent via email unless it is encrypted.
- 7.2 If any direct contact is received, relating to a Council issue, the council office should be copied into your reply.
- 7.3 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 Nazeing 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 Any mobile devices provided by Nazeing 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 Nazeing 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. Users should 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 Clerk for investigation and resolution. Report any email-related security incidents or breaches to the Clerk immediately.

13. Training and awareness

- 13.1 Nazeing Parish Council will make regular training and resources available 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 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 Nazeing Parish Council IT and email systems. By adhering to this IT and Email Policy, Nazeing Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.