Newton by the Sea Parish Council IT Policy

1. Introduction

The Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its activities and communications.

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees and volunteers in carrying out the council's business.

2. Scope

This policy applies to all individuals who use IT resources (including computers, networks, software, devices, data, and email accounts), whether their own or belonging to the council, for the council's purposes.

3. Acceptable use of IT resources and email

When using IT resources for the council's purposes, all users must adhere to ethical standards, and respect copyright and intellectual property rights. No IT resources that are provided by the council must be used to access inappropriate or offensive content.

4. Data management and security

All sensitive and confidential data that is held by the council should be stored and transmitted securely. Regular data backups should be performed to prevent data loss, and secure data destruction methods should be used when necessary.

5. Email communication

Where email accounts are provided by the council, these 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.

6. Password and account security

The council must ensure provisions are in place to enable authorised persons to have access to the council's data and accounts, whether these are on the council's or on individuals' personal IT resources. Users of IT resources for the council's purposes must maintain the security of their accounts and passwords. Passwords should be strong and regular password changes are encouraged to enhance security.

7. Email monitoring

The council reserves the right to have access to the council's email communications to ensure compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

8. 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.

9. Reporting security incidents

All suspected security breaches or incidents which relate to the council's data and accounts should be reported immediately to the council for investigation and resolution, as soon as possible.

10 Training and awareness

The council will endeavour to access periodic training and resources to educate users about IT security best practices, privacy concerns, and technology updates.

11. 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.