

Adopted 20 JULY 2026

1. Introduction

Boynton 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 councillors, employees, volunteers and contractors.

2. Scope

This policy applies to all individuals who use Boynton Parish Council's IT resources, including:

- Computers
- Networks
- Software
- Devices
- Data
- Email accounts

3. Acceptable Use of IT Resources and Email

Boynton 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 Council business
- Does not breach this policy

All users must:

- Adhere to appropriate ethical standards
- Respect copyright and intellectual property rights
- Avoid accessing inappropriate, offensive or unlawful content

4. Device and Software Usage

- Where possible, authorised devices, software and applications will be provided by the Council for official use
 - The installation of unauthorised software, including personal software, is strictly prohibited due to security risks
-

5. Data Management and Security

- All sensitive and confidential data must be stored and transmitted securely using approved methods
 - Regular data backups must be undertaken to prevent loss
 - Secure data disposal methods must be used when required
-

6. Network and Internet Usage

- Council network and internet access must be used responsibly and primarily for official purposes
 - Downloading or sharing copyrighted material without permission is prohibited
-

7. Email Communication

- Council email accounts are for official communication
- Emails must be written in a professional and respectful manner
- Confidential or sensitive information must not be sent unless appropriately secured

Users must:

- Exercise caution with links and attachments
 - Verify the source of emails before opening attachments or clicking links
 - Remain aware of phishing and malware risks
-

8. Password and Account Security

- Users are responsible for maintaining the confidentiality of their accounts and passwords
 - Passwords must be strong and not shared
 - Passwords should be changed regularly to enhance security
-

9. Mobile Devices and Remote Working

- Council devices must be protected with passcodes or biometric security
 - Remote working must follow the same security standards as office-based working
-

10. Monitoring

The Council reserves the right to monitor IT systems and email communications to ensure compliance with this policy and relevant legislation.

Monitoring will be carried out in accordance with:

- The Data Protection Act
 - UK GDPR requirements
-

11. Retention and Archiving

- Emails and records must be retained in line with legal and regulatory requirements
 - Users should regularly review and delete unnecessary emails
-

12. Reporting Security Incidents

- Any suspected IT or email security breach must be reported immediately
 - All incidents should be escalated to the Clerk to the Council for investigation and appropriate action
-

13. Training and Awareness

The Council will:

- Provide training and guidance on IT security and best practices
 - Ensure councillors, employees and relevant users are kept informed of risks and updates
-

14. Compliance and Consequences

Failure to comply with this policy may result in:

- Withdrawal of IT access

- Further action as considered appropriate by the Council

15. Policy Review

This policy will be reviewed annually to ensure it remains effective, relevant and compliant with current legislation and best practice.

16. Contacts

For IT-related queries or support, contact: **Clerk to the Council**

17. Responsibility Statement

All councillors, employees and authorised users share responsibility for maintaining the security and proper use of the Council's IT systems.

By adhering to this policy, the Council aims to maintain a secure, efficient and professional IT environment.