



IT POLICY

Drayton Parish Council

Version 1.0

Approval Date:	August 2025	Approval Route:	Council
Next Review Date:	+4 years	Document Holder:	Finance & General Purposes Committee

Document Change History

This is version 1.0 of the IT Policy and it is the responsibility of the Parish Clerk to ensure that new versions are communicated to Council and made available per the adopted Publication Scheme.

It is the responsibility of the reader to familiarise themselves with this version of the document.

This document is subject to revision and is maintained electronically. Electronic copies are version controlled and printed copies are not subject to this control.

Summary of Changes

Version 1.0 August 2025	
Ref.	Change
N/A	None

1. Introduction

Drayton 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 Drayton parish council's IT resources, including computers, networks, software, devices, data, and email accounts.

3. Acceptable use of IT resources and email

Drayton 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 Drayton 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 Drayton 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

Drayton 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 Drayton 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

Drayton 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 Drayton 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

Drayton 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 Training and awareness

Drayton 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

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

15. 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.

16. Contacts

For IT-related enquiries or assistance, users can contact the Parish Clerk.

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

DRAYTON PARISH COUNCIL
IT POLICY: SUPPORTING GUIDANCE

Policy Reference	Supporting Guidance
Acceptable use of IT resources and email	For full details on acceptable use please see HR Policy.
Device and software usage	Where Officers of the Council are provided with authorised devices, all relevant software and applications will be pre-installed. Installation of any further software and/or applications must be authorised by the Parish Clerk. Personal devices may be used to log into Microsoft 365 using Two-factor authorisation.
Data management and security	Data is stored and transmitted securely through Microsoft 365 subscription only with daily data back-up provided by Anglian Internet. For full details on secure data destruction methods please see Record Management Policy.
Network and internet usage	For full details on acceptable use please see HR Policy.
Email communication	For full details on acceptable use please see HR Policy.
Password and account security	Account management is outsourced to Anglian Internet including account access and password reset. The Parish Clerk is the nominated authorised person for Anglian Internet. Two-factor authorisation is required for all Microsoft 365 licenses.
Mobile device and remote work	For full details on acceptable use please see HR Policy.
Email monitoring	For full details on acceptable use please see HR Policy.
Retention and archiving	For full details please see Record Retention Policy.
Reporting security incidents	Designated IT point of contact is the Parish Clerk.
Training and awareness	Scheduled through the relevant Committee with responsibility for staff and Council Member training.
Compliance and consequences	For full details on acceptable use please see HR Policy.