Mapledurwell & Up Nately Parish Council

IT POLICY 2026

INTRODUCTION

1. The 2025 Practitioners' Guide introduces a requirement for an IT Policy to strengthen governance and compliance.

   Paragraph 1.54 of the Practitioners' Guide 2025 states:

   > 'All smaller authorities (excluding parish meetings) must… have an IT policy. This explains how everyone – clerks, members and other staff – should conduct authority business in a secure and legal way when using IT equipment and software. This relates to the use of authority-owned and personal equipment.'

2. As per NALC Guidance:

   > 'An IT policy helps parish and town councils set clear expectations for the appropriate use of IT equipment and systems, raise awareness of potential risks associated with IT use, safeguard the council's data and digital assets… Having a robust IT policy isn't just about compliance. It's about good governance and digital resilience.'

SCOPE

3 The Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations and communications.

4 This policy applies to council members and the clerk. By adhering to this IT and Email Policy, the Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

ACCEPTABLE USE OF IT RESOURCES AND EMAIL

5 IT and email resources are for council related activities. Users must follow ethical standards, respect copyright and Intellectual Property rights and avoid offensive or inappropriate content.

DEVICE MANAGEMENT AND SECURITY

6 All devices used for council business must have up-to-date security and antivirus protection.

DATA MANAGEMENT AND SECURITY

7 Confidential data must be stored and transmitted securely using encrypted or approved systems. Data should be regularly backed up and secure disposal procedures must be followed.

NETWORK AND INTERNET USAGE

8 Internet Usage should be responsible and efficient for official purposes. Downloading and sharing copyrighted material without proper authorisation is prohibited.

EMAIL COMMUNICATION

9 Email accounts provided by the 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.

10 Attachments and links must be treated with caution to avoid phishing and malware. Verify the source before opening any attachments or clicking on links.

PASSWORD ACCOUNT SECURITY

11 Parish Council IT users are responsible for maintaining the security of their accounts and passwords. Enable multi-factor authentication (MFA) wherever possible.

MOBILE DEVICES AND REMOTE WORK

12 Mobile devices 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.

RETENTION AND ARCHIVING

13 Emails must be retained in line with the Council's Retention of Documents and Records Management Policy and legal requirements. Non-essential emails should be deleted regularly in line with Data Protection.

REPORTING SECURING INCIDENTS

14 All suspected security breaches or incidents should be communicated immediately to all relevant parties; the clerk being the designated point of IT contact to further investigation and resolution.

TRAINING AND AWARENESS

15 The Parish Council promote awareness of IT and email security best practices, and will provide training and resources as required.

POLICY REVIEW

16 This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.