MARSKE & NEW FOREST PARISH COUNCIL

IT & EMAIL POLICY

(In compliance with Assertion 10: Digital & Data Compliance — 2025 Practitioners' Guide)

Adopted: 21st May 2026

Review Date: May 2027

---

1. Introduction

Marske & New Forest Parish Council recognises the importance of effective and secure use of information technology (IT), email, and digital platforms in supporting its operations, services, and transparency. This policy outlines the standards for acceptable use, data security, and governance.

This policy is adopted in compliance with **Assertion 10: Digital & Data Compliance** of the **2025 Practitioners' Guide**, which mandates that all local councils maintain a formal IT and digital policy.

---

2. Scope

This policy applies to:

- Councillors, employees, volunteers, contractors, and third-party providers.
- All use of council IT systems, including computers, mobile devices, software, websites, social media, cloud services, and communication platforms.
- Council email addresses and domain-based communication.
- Remote and office-based access to council data.

---

3. Acceptable Use

- IT systems and email accounts must be used for council-related work.
- Limited personal use is permitted if it does not interfere with duties, consume excessive resources, or breach this policy.
- Use of **personal email accounts** for council business is strictly **prohibited**.
- Forwarding council emails to personal accounts is not permitted.

- Accessing, distributing, or storing illegal, offensive, or inappropriate content is forbidden.

---

4. Devices and Software

- Council approved software will be provided where feasible.
- Installation of unauthorised or personal software is not allowed.
- Devices must be updated regularly with security patches and antivirus protection.
- When access ends, users must return all equipment and data.

---

5. Data Management and Security

- All data must be stored securely, using encrypted systems where necessary.
- Use of personal cloud storage for council data is **not permitted**.
- Data should be classified as public, internal, confidential, or personal, and handled accordingly.
- Regular data backups will be maintained and securely stored.
- When data is no longer required, it must be securely deleted or destroyed.

---

6. Network and Internet Usage

- Internet access must be used responsibly and primarily for council business.
- Accessing or downloading illegal, extremist, or copyright-infringing content is forbidden.
- Personal streaming, file-sharing, or excessive bandwidth use is discouraged.

---

7. Email Communication

- All council communication must be conducted via dedicated council email accounts
- **Personal accounts must not be used or linked to council business. So please note that this includes a mail forwarding service to personal email accounts.**
- Confidential information must be encrypted or sent via secure methods.

- Users must verify unknown attachments or links to avoid phishing and malware.
- Email should always be professional and respectful in tone.

---

8. Passwords and Account Security

- Passwords must be strong, unique, and not shared.
- Multi-Factor Authentication (MFA) must be used where available.
- Users are responsible for securing their accounts and updating passwords regularly.

---

9. Mobile Devices and Remote Work

- Personal devices used for council work must meet minimum security standards.
- No council data may be stored on personal devices without encryption and approval.
- Remote access (e.g. VPN) must use secure connections.

---

10. Email Monitoring

- The council reserves the right to monitor council email systems for security, legal compliance, and policy enforcement.
- Monitoring will be conducted in line with the Data Protection Act 2018 and the UK GDPR.
- Reasonable personal privacy will be respected.

---

11. Email Retention and Archiving

- Emails and digital records must be retained in accordance with legal and regulatory standards.
- Email accounts must not be used for indefinite storage — users must archive or delete data appropriately.
- Archiving and deletion must follow secure procedures.

---

12. Reporting Security Incidents

- All suspected security incidents must be reported **immediately** to the Clerk or IT provider.
- Any breach of personal data must be reported and assessed under GDPR and may require notification to the Information Commissioner's Office (ICO) within 72 hours.
- Affected parties will be informed where appropriate.

---

13. Policy Review

- This policy will be reviewed **annually**, or sooner if:
    - Legislation changes;
    - Significant new technology is adopted;
    - A data breach or security incident occurs.

The Clerk and/or IT provider will review and update the policy, with final approval by Full Council.
