# Information Technology and Email Policy

This policy reflects guidance from the Smaller Authorities' Proper Practices Panel (SAPPP 2025, Assertion 10: Digital and Data Compliance) and the NALC/Worknest HR Information Technology Policy Guidelines. It has been tailored for small parish councils using personal and council-owned devices.

## 1. Purpose and Scope

This policy sets out how all councillors, the Clerk, volunteers and contractors must use information technology (IT) and email when carrying out council business. It applies to anyone using IT systems, software, or email for Parish Council work, whether on council-owned or personal devices.

Its purpose is to ensure that all council business is conducted securely, legally, and in line with best practice, including SAPPP 2025 and the National Association of Local Councils (NALC) guidance.

## 2. Responsibilities

The Parish Clerk is responsible for ensuring this policy is communicated, implemented, and reviewed annually. The Clerk will also act as the point of contact for IT queries, data protection issues, and security incidents.

All councillors, staff, and volunteers are individually responsible for adhering to this policy.

## 3. Related Policies

This IT Policy should be read alongside the Parish Council's:

- Code of Conduct
- Data Protection and GDPR Policy
- Disciplinary Policy (for staff)
- Freedom of Information (FOI) and Transparency Code compliance documents.

## 4. Acceptable Use and Monitoring

IT systems, including email and internet access, must be used primarily for council business. Limited personal use is permitted only when it does not interfere with duties or breach council policies.

The Council reserves the right to monitor council-provided IT systems where there is a legitimate reason (e.g. safeguarding, security, or compliance). Users will be informed that monitoring may occur in line with data protection law.

## 5. Email Use Protocol

- All official correspondence must be conducted via council email addresses (e.g. clerk@croscombeparishcouncil.co.uk).
- Personal email accounts must not be used for council business.
- Generic accounts will be maintained for continuity when roles change.
- Emails must remain professional, concise, and relevant to council matters.
- Confidential or sensitive information must not be sent unencrypted.

**6. Password and Account Security**

- Passwords must contain at least 12 characters, including numbers, upper/lowercase letters, and symbols.
- Passwords must not be shared or reused across accounts.
- When an employee or councillor is absent, access to relevant systems may be granted by the Clerk for continuity of business.
- Password-protected files should have passwords shared securely (not in the same email).

**7. Computer and Device Usage**

- Computers should be logged off or locked when unattended and shut down at the end of each day.
- All files should be saved in a location accessible for backup (e.g. shared cloud drive or Clerk's master copy).
- Personal devices may be used for council work if secure, updated, and password protected (Bring Your Own Device).
- Devices used for council business must have up-to-date antivirus software and operating system updates installed.

**8. Data Protection and Privacy**

Croscombe Parish Council is a Data Controller under the UK GDPR and Data Protection Act 2018.

All personal data must be collected, processed, stored, and deleted securely and only when necessary.

Data breaches must be reported immediately to the Clerk, who will assess if notification to the Information Commissioner's Office (ICO) is required within 72 hours.

We use Mailchimp to securely store and manage the email addresses of our newsletter subscribers. Mailchimp operates under its own comprehensive GDPR compliant data protection framework, which includes encryption, secure access controls, and clear policies governing the handling and processing of personal data. We ensure that all use of Mailchimp aligns with our wider commitments to data privacy, transparency, and lawful processing.

**9. Website and Accessibility Standards**

- The Parish Council website must comply with the Web Content Accessibility Guidelines (WCAG 2.2 AA).
- Required publications include agendas, minutes, policies, AGAR, councillor details, and contact information, in accordance with the Transparency Code for Smaller Authorities.
- Accessibility and accuracy must be reviewed regularly.

**10. Cybersecurity and Social Media**

- All users must take reasonable precautions to avoid cyber risks.
- Approved antivirus software and regular updates must be maintained.
- Two-factor authentication (2FA) should be used where available.
- Only authorised personnel (the Clerk or Communications Lead) may post on official social media or website pages.
- Suspicious emails, links, or attachments must be reported immediately to the Clerk.

**11. Misuse and Disciplinary Action**

Misuse of IT facilities includes but is not limited to:

- Attempting to discover another user's password.
- Installing or running unauthorised software.
- Accessing inappropriate, illegal, or discriminatory material.
- Circumventing network security or deliberately wasting IT resources.
- Leaving laptops or devices unsecured in public places.

Any misuse may result in disciplinary or formal council action.

**12. Training and Induction**

- All councillors and staff will receive induction and annual refresher training on IT security, data protection, and responsible email use.
- Updates will be provided when legislation or best practice changes.

**13. Reporting Issues**

Any suspected security breach, data loss, or cyber incident must be reported immediately to the Clerk, who will log and investigate it and, where required, report to the ICO.

**14. Policy Review**

This policy will be reviewed annually or earlier if legislative or operational changes require. The Parish Council will minute and approve the policy each time it is reviewed.

**Policy History**

V1.0 Adopted - January 2026 (Minuted- 20 January 2026 – Ref: 149(25)a))