

IT Security and Email Best Practice for Parish Councillors & Staff

This guidance is aligned with good practice promoted by the National Association of Local Councils (NALC). It is written in clear, accessible language and is intended to support Parish Councillors and staff in meeting their statutory duties while managing IT and email securely.

Purpose of this Guidance

Parish Councillors are increasingly required to use digital systems and email to conduct council business. This document sets out simple, practical steps to help councillors:

- Meet legal and governance obligations
- Reduce the risk of cyber incidents
- Protect council information and public trust

Statutory and Governance Responsibilities

Parish Councils must operate within a clear legal and governance framework. Key responsibilities include:

- Data Protection Act 2018 and UK GDPR
- Councils must ensure personal data is handled lawfully, securely, and only for legitimate purposes.
- Freedom of Information Act 2000
- Council information must be managed, retained, and disclosed appropriately.
- Duty of Care and Proper Governance
- Councillors have a responsibility to safeguard council assets, including digital information.

Poor IT practices can undermine compliance and expose the council to financial and reputational risk.

Why IT Security Matters for Parish Councils

Parish Councils are attractive targets for cyber crime due to their role in handling public money and personal data.

Common consequences of poor IT security include:

- Financial loss or fraud
- Data breaches involving residents or staff
- Disruption to council operations
- Loss of public confidence

Email Risks and Common Threats

Email is the most common route for cyber attacks. Councillors should be aware of:

- Phishing emails designed to steal passwords or personal information
- Emails requesting urgent payments or changes to bank details
- Malicious links or attachments

Cyber criminals often rely on urgency or authority to pressure recipients into acting quickly.

Email Best Practice

To reduce risk, councillors should follow these 5 key principles:

- ✓ Use council-provided or council-approved email accounts for council business, where possible
- ✓ Use strong, unique passwords and do not share them
- ✓ Enable multi-factor authentication where available
- ✓ Check sender details carefully before responding to emails
- ✓ Avoid forwarding council emails to personal accounts unless authorised

These steps support transparency, accountability, and audit requirements.

Use of Personal Devices

Many councillors use personal devices for council work. This is acceptable provided that:

- Devices are protected with passwords or biometrics, and locked when not in use
- Operating systems and software are kept up to date
- Antivirus or built-in security tools are enabled
- Council information is not shared with other users of the device

Incident Reporting and Escalation

NALC guidance emphasises early reporting of potential issues.

If a councillor suspects a cyber or email security incident:

- Do not reply to suspicious emails
- Do not click further links or open attachments
- Report the issue immediately to the Clerk

Prompt action can significantly reduce impact and support compliance with data protection requirements.

Roles and Responsibilities

Clear roles support good governance and accountability.

Councillors must follow council policies and this guidance when using IT and email.

Clerk / Responsible Officer oversees implementation, reporting, and liaison with external support where required.

By following these simple steps, Parish Councillors can protect themselves, the council, and the community they serve.

Confirmation of Acceptance

I confirm that I have read and understood the guidance provided in this document, including my responsibilities in relation to IT security, email use, and the protection of council information.

I agree to comply with this guidance when conducting Parish Council business and to report any suspected IT or email security incidents promptly to the Clerk or Responsible Officer.

Signature: _____

Name: _____

Role (Councillor / Clerk / Staff): _____

Date: _____

Document title: IT Security and Email Best Practice

Version: 1.0

Approved by Council: xx/xx/xxxx

Minute reference: xx/xx/xxxx

Review date: March 2027

Owner: Parish Clerk