FRAMFIELD PARISH COUNCIL

INFORMATION TECHNOLOGY, DIGITAL COMMUNICATIONS AND CYBER SECURITY POLICY

A policy governing the use of information technology systems, electronic communications, social media and cyber security arrangements for Framfield Parish Council.

ADOPTED March 2026

1. Introduction

Framfield Parish Council relies on information technology and digital communication systems to support the delivery of council services, communication with residents and the administration of council business.

The Council recognises that appropriate use of information technology is essential to ensure:

- effective communication
- protection of personal and confidential information
- compliance with legal obligations
- protection of council systems from cyber security threats
- safeguarding of the council's reputation.

This policy sets out the standards expected when councillors, employees or authorised users access or use the Council's IT systems, electronic communications and digital platforms.

2. Purpose of the Policy

The purpose of this policy is to:

- establish clear expectations for the use of council IT systems and equipment
- ensure appropriate security controls are applied to protect council data
- reduce the risk of cyber security incidents
- ensure compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018
- ensure electronic communications reflect the professional standards expected of a public authority
- protect the council from legal, reputational and financial risk.

3. Effective Communication

This policy applies to:

- all councillors
- the Parish Clerk and any council employees
- contractors or authorised persons who access council IT systems
- any individual using council email addresses, devices, systems or online platforms.

The policy applies to the use of:

- council computers and laptops
- mobile phones and tablets
- council email accounts
- the parish council website
- cloud storage or document systems
- social media accounts operated by or on behalf of the council
- any personal devices used to access council systems or information.
- The policy applies regardless of whether access takes place in council offices, at home, or remotely.

4. Acceptable Use of IT Systems

Council IT equipment and systems are provided primarily for the purpose of conducting council business.

Users must ensure that:

- council equipment is used responsibly and securely
- equipment is protected from loss, theft or damage
- systems are not used for unlawful, abusive or inappropriate purposes
- confidential information is protected at all times.

Users must not:

- install software without authorisation
- attempt to bypass security controls
- access inappropriate or illegal material
- use council systems for harassment, bullying or offensive communications.

All devices used to access council systems must be protected by secure passwords and must not be left unattended when logged in.

5. Cyber Security and Information Protection

The Council recognises the increasing risk of cyber security threats to public bodies and takes appropriate steps to protect council systems and information.

Passwords

All accounts must be protected by strong passwords.

Passwords should:

- use three random words or a similarly strong format including upper, lower case alphanumeric and special characters
- not be shared with other individuals
- be changed immediately if compromise is suspected.

Where possible, **multi-factor authentication (MFA)** should be enabled.

Passwords must not be written down or stored in unsecured locations.

Devices and Portable Equipment

Devices used to access council systems must:

- be protected with a password or PIN
- have up-to-date operating systems and security updates
- be stored securely when not in use.

Loss or theft of a device containing council information must be reported to the Clerk immediately.

Data Protection

Users must comply with the Council's Data Protection Policy when processing personal data.

Personal information must not be:

- shared without lawful authority
- stored on unsecured personal devices
- transmitted through insecure channels.

Use of Online Information

Any use of publicly available online information in connection with council business must be lawful, proportionate and in accordance with the Council's Data Protection Policy.

Council systems and resources must not be used for surveillance, profiling or monitoring of individuals unless there is a clear and lawful basis for doing so.

6. Email, Internet and Digital Communications

Council email systems are provided to facilitate official communication.

Users must ensure that:

- emails are written professionally and appropriately
- confidential information is handled securely
- attachments are checked for malware before opening.

Emails should not:

- contain offensive or discriminatory material
- disclose confidential council information
- create contractual commitments without appropriate authority.

Internet use must be appropriate to council duties. Downloading and sharing illegal material or breaching copyright law is prohibited.

Retention of Digital Communications

Official digital communications, including emails and relevant social media interactions, may constitute council records and must be retained in accordance with the Council's Documents and Records Retention Policy and legal obligations.

Users must not delete, conceal or alter communications where this would conflict with the Council's duties under the Freedom of Information Act 2000 or other applicable legislation.

7. Social Media Use

Social media includes platforms such as Facebook, X, Instagram, LinkedIn, YouTube and similar online communication channels.

The Council may use social media to:

- publish council information
- advertise meetings and community events
- share information from partner organisations
- promote community initiatives.

Only authorised individuals may post content on official council accounts.

Posts must:

- be accurate and factual
- be respectful and professional
- not contain confidential or personal information.

Councillors and staff using personal accounts should ensure that personal opinions are not presented as official council views.

Users must avoid publishing content that could:

- bring the council into disrepute
- breach the Members' Code of Conduct
- prejudice council decision-making processes.

Downloading illegal material or breaching copyright law is prohibited.

Administration and Moderation

Administration and moderation of council-operated social media platforms must be carried out by authorised individuals and applied consistently, fairly and without bias.

Where content is removed or users are restricted, this must be done in accordance with the Council's adopted policies and relevant legal obligations.

8. Legal and Regulatory Responsibilities

The use of IT systems and digital communications must comply with all relevant legislation including:

- Data Protection Act 2018
- UK GDPR
- Copyright, Designs and Patents Act 1988
- Freedom of Information Act 2000
- Equality legislation
- Local Government legislation governing council communications.

Users should be aware that online communications may constitute a permanent public record.

9. Responsibility for Implementation

The Clerk will:

- oversee the security and management of council IT systems
- ensure appropriate procedures are in place
- advise councillors on compliance with this policy.

Where appropriate, the Council may engage external IT support providers to assist with system security and maintenance.

All councillors and authorised users are responsible for complying with this policy. Failure to comply may result in appropriate action being taken.

10. Contact details

Post: Framfield PC, Highlands, Blackboys, East Sussex, TN22 5LR

Telephone: 01825 890182

Email: clerk@framfieldcouncil.org.uk

11. Policy Adoption

This policy was adopted by Framfield Parish Council at its meeting on the 31st March 2026. Minor amendments can be made under authority delegated to the Clerk.

12. Document Revision History

Date	Version	Revision
02/02/2026	Draft	Final draft
10/03/2026	1.0	Final adopted version

End