Stamfordham Parish Council – IT, Email and Cyber Security Policy - May 2026

Version: May 2026 **Adopted:** May 2026 **Review Date:** May 2027

1. Introduction

Stamfordham Parish Council recognises the importance of secure, reliable and effective use of information technology (IT) to support its operations, governance, and communication.

This policy sets out the requirements for the safe and appropriate use of IT systems, email, data and devices by all users acting on behalf of the Council.

2. Scope

This policy applies to:

- Councillors
- Employees (including the Clerk)
- Volunteers
- Contractors and third parties

It covers all use of:

- Council IT systems and networks
- Email accounts
- Devices (Council-owned and personal)
- Data and information held on behalf of the Council

3. Acceptable Use

Council IT resources must be used for official Parish Council business.

Limited personal use is permitted where it:

- Is occasional and reasonable
- Does not interfere with Council duties
- Does not breach this policy or any laws

Users must:

- Act professionally and respectfully
- Comply with copyright and intellectual property laws
- Not access, store, or share inappropriate or offensive content

4. Devices and Software

Council Devices

Where provided, Council devices must be used for Council business and:

- Must not have unauthorised software installed
- Must be kept up to date with security patches
- Must have antivirus protection enabled

Personal Devices (BYOD)

Where personal devices are used for Council business:

- Devices must be password or biometrically protected
- Operating systems and apps must be kept up to date
- Data must not be stored locally unless necessary
- Devices must not be shared with others where Council data is accessible

5. Data Management and Security

All Council data must be handled securely and in line with the: •
UK General Data Protection Regulation and the

- Data Protection Act 2018.

Users must:

- Only access data necessary for their role
- Store data using approved systems (e.g. Council email, shared storage)
- Avoid storing Council data on personal drives or USB devices
- Ensure confidential data is protected at all times

Data must be:

- Backed up where appropriate
- Securely deleted when no longer required

6. Network and Internet Use

Council internet access must be used responsibly and primarily for Council business.

Users must not:

- Download or share illegal or copyrighted material without permission
- Access malicious or unsafe websites
- Introduce security risks to Council systems

7. Email Use

Council email accounts must be used for official communications.

Users must:

- Maintain a professional tone
- Avoid using personal email accounts for Council business where possible

- Ensure important Council decisions and records are retained in Council systems

Sensitive information must:

- Not be sent unless necessary
- Be protected (e.g. password-protected attachments where appropriate)

Users must remain vigilant for:

- Phishing emails
- Suspicious links or attachments

8. Passwords and Account Security

Users are responsible for protecting their accounts.

Requirements:

- Use strong, unique passwords
- Do not share passwords
- Enable multi-factor authentication (MFA) where available
- Change passwords if compromise is suspected

9. Remote Working

When working remotely:

- The same security standards apply as in an office environment
- Public Wi-Fi should be avoided or used with caution
- Devices must not be left unattended in public places

10. Email Monitoring and Privacy

The Council may monitor use of its IT systems where necessary to:

- Ensure compliance with this policy
- Protect Council systems and data
- Meet legal obligations

Any monitoring will be:

- Proportionate
- In line with the UK General Data Protection Regulation
- Authorised by the Clerk and/or Chair where appropriate

11. Retention and Record Keeping

Council records, including emails, must be retained in line with:

- Legal obligations

- The Council's document retention policy

Users must not:

- Keep official records solely in personal email accounts
- Delete records that may be required for audit, legal or FOI purposes

12. Incident Reporting

All suspected or actual security incidents must be reported immediately to:

- The Clerk (Responsible Officer)

Examples include:

- Lost or stolen devices
- Suspected phishing or malware
- Data breaches

The Clerk will:

- Investigate the incident
- Escalate where necessary (including to the Information Commissioner's Office if required)
- Take appropriate remedial action

13. Access Management (Starters and Leavers)

- Access to Council systems will be granted based on role
- Access must be removed promptly when a user leaves their role
- All Council data must be returned or securely deleted upon leaving

14. Compliance and Breaches

Failure to comply with this policy may result in:

- Removal of access to IT systems
- Further action as appropriate by the Council

Serious breaches may result in legal consequences.

15. Policy Review

This policy will be reviewed annually or earlier if required due to:

- Changes in legislation
- Emerging cyber security risks
- Changes in Council operations

16. Contact

For IT or data-related queries, contact:

Clerk to Stamfordham Parish Council

- Email: clerk@stamfordhamparishcouncil.org
- Telephone: 01669 621565
- Post: 65 Addycombe Gardens, NE65 7PE

17. Declaration

All users must confirm they have read and understood this policy.

Name:

Signature:

Role:

Date: