Stonesfield Parish Council

IT & Email Policy

1. Introduction

Stonesfield Parish Council recognises the importance of secure and effective information technology (IT) and email usage in supporting its operations, governance, and communications.

This policy sets out how IT and email should be used by councillors, employees, volunteers, and contractors to protect the Council, its data, and its reputation.

2. Scope

This policy applies to all individuals using the Council's IT resources, including computers, software, networks, email accounts, mobile devices, and cloud storage.

3. Acceptable Use

- IT resources and email accounts must be used primarily for Council business.
- Limited personal use is permitted, provided it does not interfere with Council duties or breach this policy.
- Users must adhere to ethical standards, respect copyright and intellectual property rights, and must not access or distribute offensive, inappropriate, or illegal material.

4. Devices and Software

- Where possible, authorised devices, software, and applications will be provided by the Council.
- Unauthorised installation of software is prohibited.
- Personal devices used for Council business must have up-to-date antivirus, firewall, and password protection.
- Mobile devices must be secured with PINs or biometric security.

5. Data Management & Security

- Confidential or sensitive Council data must be stored securely (e.g. encrypted drives, secure cloud storage).
- Data must only be shared via secure methods.
- Cloud storage may only be used if approved by the Council.
- Data backups should be taken regularly, and secure destruction methods used when disposing of old data.

6. Network & Internet Use

- The Council's internet and network must be used responsibly.
- Downloading or sharing copyrighted material without authorisation is prohibited.
- Users must avoid accessing malicious or suspicious sites.

7. Email Communication

- Council-provided email addresses must be used for all official communications.
- Emails must be professional, respectful, and clear.
- Confidential or sensitive information must not be sent unencrypted.
- Attachments and links should be opened only if the source is trusted.
- WhatsApp and other messaging apps may only be used where agreed by Council and for informal communications — never for statutory notices or formal records.

8. Reporting Inappropriate Communications

Any councillor or officer who receives inappropriate, offensive, or abusive communications via Council email accounts, WhatsApp groups, or other authorised platforms should report the matter to the Clerk in the first instance. Where the

complaint relates to the Clerk, the report should be made to the Chair of the Council. The Clerk or Chair will determine the appropriate action, which may include referral to the Monitoring Officer, reporting under the Council's Code of Conduct, or, if necessary, to the police.

9. Passwords & Account Security

- Users are responsible for the security of their accounts.
- Passwords must be strong, kept confidential, and changed periodically.
- Passwords must never be shared.

10. Remote Working

- When working remotely, the same security practices apply as in the office.
- Use secure Wi-Fi, avoid public/unsecured networks, and ensure screens are not visible to unauthorised persons.

11. Email Monitoring

The Council reserves the right to monitor email accounts to ensure compliance with this policy, in accordance with the Data Protection Act and UK GDPR.

12. Retention & Archiving

- Emails and electronic records must be retained in line with statutory and regulatory requirements.
- Unnecessary emails should be regularly deleted to maintain an organised system.
- Statutory documents must be filed appropriately and kept accessible.

13. Procurement & IT Services

- Any new IT systems or software must be approved by Full Council before purchase.

- Contracts and licences should be recorded, monitored, and renewed appropriately.

14. Reporting Security Incidents

- Any suspected data breach, IT security incident, or loss of equipment must be reported immediately to the Clerk (as Data Protection Officer) for investigation.

- Incidents may also need to be reported to the ICO (Information Commissioner's Office) within statutory timeframes.

15. Training & Awareness

- The Council will provide training to councillors and staff on IT security, safe email use, and data protection.

- Awareness will be refreshed annually or when new risks are identified.

16. Compliance & Consequences

- Breaches of this policy may result in suspension of IT privileges, referral to the Monitoring Officer, and/or further action as considered appropriate by the Council.

17. Policy Review

This policy will be reviewed annually, or sooner if required due to legislative or technological changes.

Date adopted: June 2025
Review date: 1st October 2025

This is a revised draft of the Council's IT & Email Policy. This version keeps all of the parish-specific provisions from our June 2025 policy (e.g. WhatsApp use, cloud storage, procurement rules) but also incorporates additional best practice elements that have been introduced since June, including:

- Acceptable use principles (copyright, offensive material, ethical standards)

- Device/software usage rules (no unauthorised installations)
- Clearer password/account security (no sharing, stronger controls)
- Network & internet usage
- Remote working and mobile device security
- Email monitoring (GDPR-compliant)
- Retention & archiving of emails/documents
- Reporting IT security incidents (not just data breaches)
- Training & awareness commitments
- Compliance & consequences of breaches

Adopted: July 2025
Reviewed: October 2025