

Sutton Parish Council

IT, Email & Cyber Security Policy

Version1

Review Frequency: Annual

Approved by: Sutton Parish Council

Date Approved: 11th December 2025

1. Purpose

This policy ensures the secure, lawful and effective use of information technology (IT), email communication, digital data and online systems by Sutton Parish Council. It aims to protect the Council from cybersecurity threats, ensure compliance with data protection legislation, maintain transparency and safeguard public information.

2. Scope

This policy applies to:

- All councillors
- The Clerk
- Council employees
- Contractors, third parties or volunteers who access or handle Council data

3. Legal Compliance

All IT and email use must comply with the following legislation:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Human Rights Act 1998
- Defamation Act 2013
- Local Government Act 1972

4. Roles and Responsibilities

The Clerk is responsible for IT administration, access control, and reporting IT security incidents.

All users must:

- Use IT and email responsibly
- Protect Sutton Parish Council data from unauthorised access
- Report any security incidents immediately
- Follow this policy at all times

5. Acceptable use of IT resources and email

Sutton Parish Council IT resources and email accounts are to be used for official council business. Limited personal use is allowed if it does not:

- Affect council work
- Incur cost
- Breach policy or law
- Users must not access, view, store or share any **offensive, extremist, abusive, pornographic, discriminatory or illegal content**

6. Device and software usage (BYOD – Bring Your Own Device)

Councillors and the Clerk may access council email and documents on personal devices only if it can be ensured that they are covered by the Councils publication scheme:

- The device is password or passcode protected
- It has antivirus or security updates enabled
- Sutton Parrish Council data is not stored permanently on the device
- The device can be wiped if lost or stolen

Only secure and approved applications may be used to access or store Sutton Parish Council information. Personal devices may contain other software, but Sutton Parish Council information must not be stored in unapproved apps or services (e.g. personal Dropbox, WhatsApp, Messenger, or personal email). Council data must only be accessed using trusted software and secure cloud storage approved by the Clerk.

7. Data management and security

All Sutton Parish council data must be stored securely in a **council-approved cloud storage location**. Personal email accounts must not be used for council business. Confidential or sensitive data must be stored securely and encrypted if necessary. USB drives are **not permitted** unless encrypted and approved by the Clerk.

8. Network and internet usage

Sutton Parish Council's Council systems must be used responsibly and for lawful purposes.

Users must not:

- Download illegal or harmful material
- Bypass security systems
- Risk of cyber infection by clicking unknown links

9. Email communication

• **Zoho Mail** is the approved Sutton Parish Council email system. Email accounts provided by Sutton Parish Council are for official communication only.

- Emails should be professional and respectful in tone.
- Confidential or sensitive information must not be sent via email unless it is encrypted.
- Users must check sender identity before opening attachments (phishing protection)

10. Password and account security

- Sutton Parish Council users are responsible for maintaining the security of their accounts and passwords.
- Passwords should be strong and not shared with others. Regular password changes are encouraged to enhance security.
- Zoho Mail is created with multi-factor authentication (MFA) it is responsibility of councillors to keep their back-up codes for their Zoho Mail Account.
- Report suspected password compromise to the Clerk immediately

11. Mobile devices and remote Work

Mobile devices provided by Sutton Parish Council should be secured with passcodes and/or biometric authentication. When working remotely, users should follow the same security practices as if they were in the office.

- Devices must be locked when unattended
- Public Wi-Fi must not be used without secure protection

12. Email monitoring

Sutton Parish Council reserves the right to monitor email communications to ensure

- Security
- Compliance &

- Legal obligations

Compliance with this policy and relevant laws. Monitoring will be conducted in accordance with the Data Protection Act and GDPR.

13. Use of Messaging and Social Media

- WhatsApp, Facebook Messenger and SMS must **not** be used for council decision making
- Council documents must **not** be shared unofficially online
- All official business must be conducted via council email
- **The Parish Council Social Media & Communications Policy** must be followed

14. Retention and archiving

Emails should be retained and archived in accordance with legal and regulatory requirements. Regularly review and delete unnecessary emails to maintain an organised inbox. Members must not delete records that may be required for Freedom of Information (FOI).

15. Reporting security incidents

All suspected security breaches or incidents should be reported immediately to the Clerk including

- Phishing Emails
- Lost or Stolen Devices
- Cyber-attacks or suspicious activity
- Data breaches

The Clerk will investigate and report to the ICO if required.

16. Training and awareness

All councillors and staff must complete basic cyber security and data protection training annually.

17. Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges and formal investigation by the Monitoring Officer and if deemed necessary any further action.

18. Policy review

This policy will be reviewed annually to ensure its relevance and effectiveness. Updates may be made to address emerging technology trends and security measures.

19. Contacts

For IT-related enquiries or assistance, users can contact the Parish Clerk.

All staff and councillors are responsible for the safety and security of Sutton Parish Council's IT and email systems. By adhering to this IT and Email Policy, Sutton Parish Council aims to create a secure and efficient IT environment that supports its mission and goals.

11th December 2025

Date: _____

Mrs S Giller

Signature: _____

Parish Clerk and RFO

Role: _____

Appendix A – Password Security Standards

- Minimum 12 characters
 - Use upper and lowercase letters, numbers and symbols
 - Do not reuse passwords
 - Do not write passwords down
 - Copy Zoho back-up codes and keep in a safe place
-

Appendix B – Personal Device Security Checklist (BYOD)

- Device locked by passcode or fingerprint
 - Screen timeout enabled
 - Antivirus active
 - Updates installed regularly
 - Council data is not stored permanently
 - Lost or stolen devices are reported immediately
-

Appendix C – Cyber Incident Procedure

If you suspect a cyber-attack:

1. Stop work immediately
2. Disconnect the device from the internet
3. Do not delete anything
4. Report it to the Clerk immediately
5. Await further instructions