Sutton Parish Council

IT POLICY 2025

ADOPTED 22nd July 2025

CONTENTS

Action	Reviewed By	Version/Date Adopted/Minute Ref
Review by Full Council 22nd July 2025	Reviewed and approved by Full Council	V1, Min Ref 067/25(a)
Next Review July 2028		

1. Purpose & Scope

This policy defines how Sutton Parish Council manages its use of information technology, in line with the Transparency Code for Smaller Authorities (2015) and the 2025 edition of the Practitioners' Guide. It ensures the council's digital operations are transparent, secure, and compliant with data protection laws.

This policy applies to all **councillors**, **employees**, **volunteers**, and **contractors** who access or manage the council's IT resources, including but not limited to:

- Desktop and laptop computers, tablets, and smartphones
- Email and cloud-based systems
- Council website, social media, and digital publication tools
- Video conferencing and messaging platforms
- Personal devices used under Bring Your Own Device (BYOD) provisions

2. Introduction

1.1 The Council has a duty to ensure the proper security and privacy of its computer systems and data. All users have some responsibility for protecting these assets.

1.2 The Clerk is the designated Data Protection Officer (DPO) and IT Systems Administrator and is responsible for the implementation and monitoring of this policy but may delegate that responsibility to another officer.

1.3 Line managers have a responsibility to ensure that the staff they supervise comply with this policy

3. Governance and Oversight

All processing of personal data shall comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

a. General

- All employees, members and other users of Council IT equipment must be familiar with and abide by the regulations set out in the Council's 'Privacy Policy'.
- All data collection, processing, and subject rights are governed by the council's Privacy Policy, and is available on the council website.
- Data must be stored securely, with access granted only to authorised personnel based on necessity.

- Personal data will be retained in accordance with the council's Data Retention Schedule and securely deleted when no longer needed.

- All council devices will have up-to-date antivirus software installed and this must not be switched off for any reason without the authorisation of the Parish Clerk.
- All council devices should be password protected to prevent unauthorised access.
- Password protection and multi-factor authentication where applicable
- Regular updates and anti-malware software
- Backups of essential data in secure locations
- All users are reminded that deliberate unauthorised use, alteration, or interference with computer systems, software or data is a breach of this policy and in some circumstances may be a criminal offence under the Computer Misuse Act 1990.
- All users should ensure that portable equipment is properly locked away when not in use and computers are locked if being left on.
- All software installed on council devices must be fully licensed

b. Use of Personal Devices (BYOD)

- Councillors and staff may use personal devices to access Council systems only if explicitly authorised and subject to compliance with this policy.
- Devices must be protected by strong passwords, encryption (where possible), and up-to-date antivirus software.
- Access to council data on personal devices must be controlled and subject to regular review.
- Council data must be kept separate from personal data using dedicated apps or storage areas.

c. Emails

- The use of personal email accounts for council business is strictly prohibited. All council correspondence must be conducted through official council-provided email addresses.
- Emails from council-owned domains must not be forwarded to personal email addresses.
- Any breaches will be investigated, and appropriate measures taken in line with the council's disciplinary or governance procedures.
- All council emails will be stored in compliance with the GDPR and Freedom of Information requirements.

d. Employees & Members

- The Clerk will assign employees and Members a Council e-mail address as appropriate
- Personal use of Council IT equipment is permitted but should be kept to a minimum during working hours. Reasonable use of the internet during working hours is permitted.
- Software should not be installed without the authorisation of the Parish Clerk
- Members are reminded that any e-mail sent or received in their capacity as a Parish Councillor is Council data and any e-mails may have to be disclosed following requests under the Data Protection Act or Freedom of Information Act. This includes e-mails on Personal Accounts when acting as a Councillor.
- A copy of all e-mail received on the Councillor e-mail accounts is kept on the server
- A copy of all e-mail sent from Councillor e-mail accounts on the webmail is kept on the server; it is recommended that members not using webmail to access e-mail should set up a rule to ensure a copy of e-mail is kept on the server.

e. Social Media

- Social Media (such as Facebook and Twitter) may be used by the Parish Council as part of its means of communication with the community
- All general social media will be operated by council officers
- All council social media messages must be non-political, uncontroversial and used to promote/highlight the Parish.
- Members using social media in their capacity as councillors must make it clear they are speaking in a personal capacity and not representing the view of the Council.
- Members should ensure they are adhering to the Council's code of conduct when using social media.

f. Council Website(s)

- Council officers should ensure any websites operated by the council are kept up-to-date
- Officers must ensure that the most up-to-date version of the Members' Register of Interests is uploaded to the website
- The website will be monitored for unauthorised access and abuse

g. Misuse & Data Breaches

The Parish Council is committed to responding promptly and effectively to any data breaches to minimise risk and comply with UK GDPR requirements.

A data breach is a security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include:

- Loss or theft of devices containing personal data
- Unauthorised access to council email accounts or files
- Sending personal data to the wrong recipient

- Malware or ransomware attacks compromising council systems

All misuse is prohibited including specifically, but not exclusively the following:

- Creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material
- Creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission of defamatory material
- Transmission of material which in anyway infringes the copyright of another person
- Transmission of unsolicited commercial advertising material to networks belonging to other organisations
- Deliberate actions or activities with any of the following characteristics:
    a. Wasting staff effort or networked resources
    b. Corrupting or destroying another users' data
    c. Violating the privacy of other users
    d. Disrupting the work of other users
    e. Other misuse of the networked resources by the deliberate introduction of viruses/malware
    f. Playing games during working hours
    g. Altering the set up or operating perimeters of any computer equipment without authority.

- Any councillor, employee, or contractor who becomes aware of a data breach must report it immediately to the Clerk (Data Protection Officer).
- The Clerk will assess the severity and scope of the breach and determine if mitigation steps are required (e.g., changing passwords, disabling access, enabling 2FA).
- A full investigation will be conducted by the Clerk or designated officer within 72 hours of the breach being discovered.
- The breach will be logged, including:
    I. Date and time of breach
    II. Type and volume of data affected
    III. Cause and extent of the breach
    IV. Actions taken to address the breach

If the breach is likely to result in a risk to the rights and freedoms of individuals, the council must notify the Information Commissioner's Office (ICO) within 72 hours.

* If the breach poses a high risk to the individuals affected, those individuals must also be informed without undue delay, outlining:

- The nature of the breach
- Likely consequences
- Measures taken to mitigate the risk

- Contact information for further support

h. Training and Policy Review

All devices must be regularly updated and checked for compliance with this policy.

Users will be given training on IT systems, cybersecurity, data handling, and transparency responsibilities.

This policy will be reviewed annually, or sooner if legislation or requirement changes.

Periodic internal audits will check for compliance with security and transparency requirements.