

Sutton Benger Parish Council - Information Technology Policy 2025

As Adopted at the Parish Council Meeting held on 8th October 2025 – Minute No. 136.25

Introduction

Sutton Benger Parish Council recognises the importance of effective and secure Information Technology (IT) systems and email usage in supporting the communication required to run an efficient and responsive Parish Council.

Scope of Policy

This IT Policy provides guidelines and responsibilities for the appropriate use of the IT resources provided by the Parish Council and all methods of electronic communication made in the course of Parish Council business, including the Internet, social media and the use of email. The policy applies to the activities of both parish councillors (**members**) and the Parish Clerk/Responsible Financial Officer (**officer**).

Objectives

Parish Council business is highly reliant on effective electronic communications and processing of information. The objectives of this policy are to:

- Minimise risks of disruption, delay or compromise to council business.
- Protect confidential and sensitive information.
- Ensure compliance with legally mandated requirements including data protection and freedom of information with the minimum of extra effort.

Use of Technology

The Council makes use of IT systems for data storage, communications and as a source of information. Where hardware and software are provided by the Parish Council, this Information Technology policy has also been adopted to:

- Prevent inappropriate use of computer equipment (such as extended personal use)
- Protect confidential, personal or sensitive data
- Prevent the introduction of malware, e.g., viruses
- Prevent the use of unlicensed software
- Prevent the access and circulation of inappropriate (e.g., racist, sexist or defamatory) material
- Ensure that Council property is properly looked after

Parish Council e-mail addresses

All councillors and the Parish Clerk will be provided with a gov.uk e-mail address to use specifically for official council business and use of personal e-mail accounts for parish council business is strongly discouraged. Using a gov.uk e-mail is recommended for enhanced security and professionalism and clearly delineates any communication undertaken on behalf of the Parish Council from that of the individual. It also helps with compliance with regulations like GDPR and Freedom of Information requests and prevents an individual from being obliged to permit access to information stored within their own computers, electronic devices and e-mail accounts. Members will be required to surrender their gov.uk email account and all of its contents to the Parish Clerk when they leave the Council. In the event of the Parish Clerk/RFO leaving, they will be required to surrender their e-mail account to the Chair of the Parish Council or their nominated representative.

Passwords

Protecting access to a member's e-mail address is the responsibility of each individual. Essential actions include putting in place adequate security measures to protect digital information from unauthorised access.

This involves creating strong passwords and using them correctly. If a member or the Parish Clerk/RFO believes that someone else knows their password, they must ensure that the password is changed immediately. If password protected documents are emailed, care should be taken to communicate the password to the recipient in an equally secure way over a different medium.

Social Media

This policy includes social media and online participation in, for example, forums, blogs, and non-Parish Council websites in relation to Parish Council business.

Members and the Parish Clerk/RFO using their own social media accounts in any matter that might be considered to relate to Parish Council business must ensure that any comment made is clearly identified as their own and not as a representative of the Council.

Members and the Parish Clerk/RFO may not disclose personal information about Parish Council members unless expressly authorised to do so.

No member or officer may create, communicate or share anything of an offensive nature, including defamation or harassment of colleagues or others when acting on behalf of the Parish Council. This will be considered as bringing the Parish Council into disrepute.

Members and the Parish Clerk/RFO using social media in any capacity should always be aware of their association with the Council and make sure that any use of social media is consistent with this.

Use of Parish Council-related facilities

All members and the Parish Clerk/RFO are expressly prohibited from using the Parish Council's facilities (hardware or e-mail addresses) for the sending, receiving, printing or otherwise disseminating information which is the confidential information of the Parish Council or associated organisations, other than in the normal and proper course of carrying out duties for the Council.

Use of Laptop Computer

The Parish Council provides a laptop computer for the use of the Parish Clerk/RFO. This facility must be used for Parish Council business purposes only. The device and devices associated with it are recorded on the Asset Register and covered by the Parish Council's insurance policy as part of its risk management.

To maintain the confidentiality of information held on or transferred via this computer, security measures must be followed at all times. The computer should be protected by a log-on ID and password which should be changed regularly and must be kept secure. Before moving the computer (e.g., offsite to Parish Council meetings) or leaving the computer for long periods of time or overnight the computer should be fully shut down.

Laptop Computer Safety

It is the responsibility of the officer who has been provided with a Parish Council laptop computer to take all reasonable precautions to safeguard their device and the information contained on it. This includes protecting it from physical hazards, including spilling liquids; not allowing unauthorised users access to the machine; leaving the device in a vulnerable place, such as a car; and making sure they adhere to this policy.

Laptop Computer Backup

In order to ensure proper back up of data on the Parish Council's computer, all files must be stored on the iCloud [or OneDrive] and on a 6-monthly basis, backed up to an external hard drive which is stored in a locked safe at the Parish Clerk/RFO's home.

Software

The Parish Council is committed to using software for which it is properly licensed, following the terms of all software licences to which it is a contracting party, and will not accept the use of unlicensed software or more copies of software than it has licences for.

This means that software must not be installed onto the Parish Council computer unless the appropriate licence has been obtained, that the software is virus free and that it is compatible with the computer's other facilities.

In Case of Emergency (Parish Council Officer)

All passwords that the Parish Clerk/RFO holds and which are required to access the officer's laptop, Parish Council data and related backups should be provided to the Chair or his nominated representative in a secure file and updated on a 3-monthly basis. This file should only be accessed in the event that the officer is unable to carry out their duties for medical or personal reasons for a period of time likely to be longer than 2 weeks.

This also applies to any passwords that the Parish Clerk, as Responsible Financial Officer, uses to carry out their role (e.g., bank accounts, HMRC, etc.).

In the event that a member is likely to be unavailable for a long time (e.g., if they are off on long-term sick), consideration should be given to forwarding their e-mails to another member or officer, particularly in relation to their allocated council responsibilities.

Website and e-mail Maintenance – Access, Maintenance and Backup

The councillor responsible for administering the Parish Council website and email accounts should ensure that one other person (either the officer or another councillor) is able to carry out website and email administration and has the same permissions and functionality as themselves.

All procedures should be documented and this document updated should procedures change.

Personal Use and Responsibility

The Parish Clerk/RFO is required to return all business-related IT equipment, records and documents in their possession if they leave the Parish Council. Failure to return identified equipment may be a breach of security and action taken. They may also be required to surrender their e-mail account unless arrangements have been made to hand over the same e-mail address to their successor as part of their handover process.

If any member receives an offensive communication through their gov.uk email account or via a Parish Council related on-line resource, they should inform the Parish Clerk/RFO, or in the event such a communication is received by the officer, they should inform the Chair. In such circumstances any such message should not be deleted from any storage system unless instructed to do so. Depending on the nature of the communication, an investigation may be carried out (including informing the police if appropriate).

System Security

Members and the Parish Clerk/RFO must keep all passwords and security codes secure.

Members and the Parish Clerk/RFO are personally responsible for all their activity using any IT system or service for Parish Council business.

Members and the Parish Clerk/RFO should take precautions to stop unauthorised use of their login credentials by not writing them down and ensuring they lock any device when it is being used for Parish Council business if leaving it unattended even for a short time.

Legislation

All Sutton Benger Parish Council information and data is subject to the General Data Protection Regulation (2018), and Data Protection Act (2018).

In the event that the Parish Council receives a Freedom of Information Request (FOI), under the Freedom of Information Act (2000), all IT systems and devices provided by the Parish Council may be searched for the requested information.

Members and the Parish Clerk/RFO will be informed that this needs to occur prior to any search taking place.

Equality and Diversity

The Parish Council recognises its responsibilities and legal obligations under the Equality Act (2010) and will endeavour to respond with reasonable modifications to IT equipment and services if required.

Any member or officer having physical difficulties with the use of IT equipment and services, should in the first instance consult with the Parish Clerk/RFO, who, in consultation with the Chair, may contact the Wiltshire Association of Local Councils (WALC) to establish whether an assessment should be carried out in order to facilitate the member or officer with carrying out their role as easily as possible.

Review

This policy will be reviewed every three years by the Parish Council, unless changes become needed on a more urgent basis. Feedback from members and the Parish Clerk/RFO and information gained from the monitoring of the policy will be used to improve the policy.