

St Sampson Parish Council

IT Policy

The 2025 edition of the Practitioners Guide contains a new Assertion 10 covering digital and data compliance. In addition to requirements related to email management and website accessibility, there is a new requirement for smaller authorities (excluding parish meetings) to have an IT Policy (1.54).

This document states the IT Policy of St Sampson Parish Council.

Introduction

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

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources, online services and email by Council members and employees eg the Clerk.

Scope

This policy applies to all individuals who use IT resources, including computers, networks, software, devices, data, email and other online accounts. Whilst the Clerk is provided with IT resources, the Council acknowledges that members will be using their own personal devices. Everyone must adhere to this policy to maintain digital security.

Training and awareness

Individuals are expected to engage in regular training on email security and best practices, in particular:

1. the Parish Council Domain Helper Service's virtual cybersecurity workshops for Councils
2. the National Cyber Security Centre Cyber Security training for small organisations and free Cyber Action Toolkit.

If additional training about IT security best practices, privacy concerns, and technology updates is required please consult with the Clerk.

Acceptable use of Council provided IT resources

When using IT resources for the Council's purposes, individuals must adhere to ethical standards, and respect copyright and intellectual property rights.

When using any device on Council business, individuals must make sure they are:

- i. using strong passwords for all Council supplied accounts, including email (preferably using a password manager)
- ii. downloading/installing the latest security updates for the operating system and relevant applications
- iii. using anti-virus protection

Council provided IT resources and email must never be used to access or forward inappropriate or offensive content.

Where the Council has provided individuals with devices to use for Council business they should be used in preference to personal devices. Unauthorised software must not be installed on Council provided devices without first checking with the Clerk.

Network and internet usage

Individuals must be careful about which Wi-Fi networks they join. Public Wi-Fi networks in coffee shops or on trains can be targeted by hackers. In preference use a trusted internet connection, which is password protected when carrying out official business.

Password and account security

Individuals are responsible for maintaining the security of their accounts and passwords. Use the National Cyber Security Centre's advice for choosing a strong password. For business continuity, login details and passwords for accessing Council provided devices need to be stored securely so they can be accessed by trusted individuals in an emergency.

St Sampson Parish Council IT Policy

Email communication

The Council provides members and the Clerk with an official email account for organisation-related communication only. Individuals must make sure that emails are professional and respectful in tone. Always check confidential or sensitive information is only sent to the correct recipients.

Always be cautious when downloading attachments and opening links to avoid phishing and malware. Before opening any attachments or clicking on links, verify the source by looking at the email it has come from carefully. Do not download and open anything if unsure who has sent it.

Email access

The Council reserves the right to check email communications to ensure compliance with this policy and relevant laws. Any checking undertaken will be conducted in accordance with the Data Protection Act and GDPR. Clerks may need to access emails so that they can respond to FOI or subject-access requests. If using a personal email account for Council business, be aware this is still subject to data protections laws and FOI requests.

Data management, data retention and security

All sensitive and confidential data should be stored and transmitted securely. Individuals must regularly backup any important data to prevent data loss and follow the Council's data retention policies.

Individuals should retain and archive emails in compliance with the Council's data retention policies. Regularly review and delete unnecessary emails to maintain an organised inbox.

Reporting security incidents

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

Compliance and consequences

Breach of this IT and Email Policy may result in the suspension of IT privileges.

Date of adoption: _____ at a meeting of the Council as minuted 12



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