SOUTH WONSTON PARISH COUNCIL INFORMATION TECHNOLOGY POLICY

This is South Wonston Parish Council's Information Technology (IT) Policy. Its purpose is to ensure all users understand how to use Parish Council hard and software appropriately and responsibly, how to manage the handling and safekeeping of data and which are the relevant Parish Council policies and UK Government laws. This IT Policy applies to employees, councillors and third parties (volunteers, contractors and hirers of Parish Council facilities). The IT covered by this policy includes the Parish Office computer and its system and application software, the webmail, website and Hallmaster Booking System, the Wi Fi and CCTV hubs, and the office smart phone. Hardware is listed on the Asset Register. IT provision is assessed annually through the requirements of the Risk Management and Register Policy. IT problems may be made known via Clerk to the Parish Council's IT adviser. Regular monitoring and an annual review of this policy will be carried out by Clerk and a nominated councillor to ensure relevance and effectiveness. Updates to address emerging concerns and security measures will be put in place as required.

PASSWORDS

Passwords are created to be as strong and secure as possible, using a combination of letters, numbers and symbols. They remain the property of the Parish Council and may not be divulged unless Clerk is absent or unwell, in which case the Chair or Vice Chair may request the password for the office computer, or if a councillor should need the Clerk's password to access the website of a professional organisation to which the Parish Council belongs for official purposes. Users of Parish Council webmail are responsible for the security of their passwords, but if a councillor believes that their webmail password has been stolen by bad actors, they should report to Clerk who will alert the provider of the webmail to the need for investigation. The Wi Fi password must not be shared insecurely. Users of the Hallmaster Booking System are also responsible for the security of their passwords.

OFFICE COMPUTER USAGE

The office computer remains the property of the Parish Council and at the end of Clerk's employment it will be returned to the Parish Council OR at the end of Clerk's employment, her property will have all Parish Council data removed.

If moving away from the Office, Clerk will log out and lock the office door to protect the computer, the phone, if not taken, and the CCTV monitor. On leaving for home, Clerk will keep the computer securely indoors and not leave it, even if secured out of sight, in a locked vehicle. If working at home, Clerk will observe similar security practices.

RISK MANAGEMENT

What are the risks to IT equipment? These could be loss through accidental damage, fire or theft and the accidental or malicious loss of system and application software. In addition, breaches of data protection, privacy, copyright and rights may occur. The Parish Council's preventive procedures will include insurance for IT equipment, regularly reviewed and adjusted, fire and security alarms with codes, naming

protocols for files and passwords, and back up of files, document scanning, secure storage and anti-virus software as part of Business Continuity measures in the Risk Management Policy and Register.

USE OF PRIVATE IT

The Parish Council does not supply councillors with IT equipment. Councillors may use their own devices in meetings and for official correspondence by council webmail in accordance with Parish Council Policies and Code of Conduct. Similar practices must be observed at home when undertaking council work. Correspondence subject to a Freedom of Information Request must be retained until no longer needed; other emails should be dealt with according to the Retention of Documents Policy. On resignation or retirement, councillors must delete all Parish Council records.

DATA PROTECTION

The guidelines set out in the Data Protection Policy must be followed by everyone processing personal data.

MOBILE PHONE TEXTING

Clerk may use the office phone for business text messages. Other users may send official text messages from their private mobile phones. All must observe policy and legal requirements.

EMAILS.

Councillors are responsible for their official emails which should always reflect Parish Council decisions and policies. Parish Council email addresses must not be used for private correspondence. Mail sent to a councillor’s private email address regarding council matters by a non-council sender must be re-directed. Mail in inboxes which is no longer relevant must be deleted.

INTERNET USE

Clerk alone may use the office computer for internet access and is solely responsible for downloading software. Councillors and users of the Wi Fi connection can use their own devices appropriately. The Wi Fi network will be secured to prevent connected devices from compromise and the password shared safely.

TRAINING

Courses on information security will be made available as required.

MISUSE OF IT AND PENALTIES

See Standing Orders, Data Protection, Social Media, Complaints and Persistent Complainant Policies and Code of Conduct.

RELEVANT LEGISLATION

Data Protection Act 2018 and UK General Data Protection Regulations 2021.

Data Use and Access Act 2025.

Communications Act 2003.

Malicious Communications Act 2003.

Online Safety Act 2023.

Copyright, Designs and Patents Act 1988

Human Rights Act 1998.

RELEVANT SOUTH WONSTON PARISH COUNCIL POLICIES

Standing Orders 2024

Code of Conduct 2025

Risk Management and Register Policy 2024

Retention of Documents Policy 2023.

Correspondence Policy 2024

Social Media Policy 2024

Complaints Policy 2024

Persistent Complainants Policy 2024

DATE OF ADOPTION

DATE OF REVIEW