# SOUTHWATER PARISH COUNCIL

## IT POLICY

| | |
|---|---|
| Reviewed: | N/A - New Policy |
| Approved: | F&GP Committee 15th October 2025 |
| Review Period: | Annually |
| Next Review Date: | October 2026 |

# INDEX

## Contents

# 1. Introduction

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

This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and contractors.

Southwater Parish Council is accredited under the **UK Government's Cyber Essentials scheme**, demonstrating a baseline of robust cyber security measures. The Council commits to maintaining this accreditation through annual renewal as part of its ongoing commitment to digital and data compliance, resilience, and the protection of personal data.

# 2. Scope

This policy applies to all individuals who use Southwater Parish Council's IT resources, including computers, networks, software, mobile devices, data, and email accounts.

# 3. Acceptable Use of IT Resources and Email

Southwater Parish Council IT resources and email accounts are to be used for official Council-related activities and tasks. Limited personal use is permitted, provided it does not interfere with work responsibilities or violate any part of this policy.

All users must:

- Adhere to ethical standards.
- Respect copyright and intellectual property rights.
- Avoid accessing inappropriate, offensive, or illegal content.

# 4. Device and Software Usage

Where possible, authorised devices, software, and applications will be provided by Southwater Parish Council for work-related tasks.

Unauthorised installation of software (including personal applications) is prohibited. Only licensed software approved by the Council may be used.

# 5. Delegated Authority

The Executive Officer, as Proper Officer to Southwater Parish Council, has delegated authority to approve, procure, and manage IT devices, software applications, and digital systems

required for the effective administration of the Council, provided that expenditure is within the approved annual budget or within the Executive Officer's delegated financial limits under the Financial Regulations.

The Executive Officer will ensure:

- Compliance with Standing Orders and Financial Regulations
- Consistency with the Council's Cyber Essentials accreditation standards.
- They seek professional advice and/or advice from the IT Services and Support Provider if further guidance or clarity is required on IT related matters.

## 6. Data Management and Security

- All sensitive and confidential Southwater Parish Council data should be stored and transmitted securely using approved methods.
- Regular data backups should be performed to prevent data loss.
- Secure methods of data destruction must be used where necessary.

As a Cyber Essentials accredited organisation, Southwater Parish Council ensures that its systems meet Government-backed minimum standards for firewalls, secure configuration, user access control, malware protection, and patch management.

Southwater Parish Council maintains a Data and Information Asset Register, which records all datasets and information assets held by the Council, their purpose, lawful basis for processing, retention periods, storage arrangements, and security controls.

The Register forms part of the Council's compliance framework for UK GDPR, the Data Protection Act 2018, and Assertion 10 of the Annual Governance and Accountability Return (AGAR). It is reviewed annually by the Executive Officer to ensure it remains accurate and up to date.

## 7. Network and Internet Usage

Southwater Parish Council's networks and internet connections should be used responsibly and efficiently for official purposes.

- Downloading or sharing copyrighted material without authorisation is prohibited.
- Streaming, gaming, or non-work use that impacts security is not permitted.

## 8. Email Communication

- Council-provided email accounts must be used for all official correspondence.
- Emails should be professional and respectful in tone.
- Confidential or sensitive information must not be sent via email unless encrypted.
- Caution must be taken with attachments and links to avoid phishing or malware.
- Verify the source before opening any attachments or clicking on links.

## 9. Password and Account Security

- Southwater Parish Council users are responsible for maintaining the security of their accounts and passwords.
- Passwords should be strong, unique, and must not be shared with others.
- Multi-factor authentication (MFA) should be used where available.
- Password changes may sometimes be encouraged to enhance security (as advised by the Council's IT Services and Support provider).

## 10. Mobile Devices and Remote Work

Mobile devices provided by Southwater Parish Council (if issued) 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.

## 11. Email Monitoring

The Council reserves the right to monitor email communications to ensure compliance with this policy and with relevant laws. Monitoring will always be undertaken in accordance with the Data Protection Act 2018 and UK GDPR.

## 12. Retention and Archiving

Emails and electronic records must be retained and archived in line with the Council's Retention and Disposal of Documents Policy and in accordance with legal and regulatory requirements.

Regularly review and delete unnecessary emails to maintain an organised inbox.

## 13. Reporting Security Incidents

All suspected security breaches, data losses, or cyber incidents must be reported immediately to the Executive Officer (or their delegate) for investigation and resolution.

Any breach involving personal data will be managed in accordance with the Council's Information Security Incident Policy and, where required, reported to the ICO within statutory timescales.

## 14. Training and Awareness

All employees, councillors, and volunteers handling personal data or using Council IT systems must undertake data protection and IT security training at least once every three years (or more frequently if legislation or best practice requires).

Training will include:

- Data protection principles (UK GDPR / DPA 2018).
- Cyber security awareness (phishing, malware, safe use of devices).
- Information governance responsibilities.

Attendance records will be maintained as audit evidence.

## 15. Related Policies

This IT Policy should be read alongside the Council's other adopted policies, which together form the Council's governance framework for information management and digital compliance:

- Data Protection Policy
- Data Protection (of Staff) Policy
- Information Security Incident Policy
- Freedom of Information Policy
- Members Correspondence Policy
- Retention and Disposal of Documents Policy

## 16. Compliance and Consequences

Breaches of this policy may result in suspension of IT privileges, disciplinary action, further consequences as deemed appropriate, or referral to relevant authorities where necessary.

## 17. Policy Review

This policy will be reviewed annually to ensure continued relevance and effectiveness, including to confirm renewal of Cyber Essentials Accreditation. Updates will be made to reflect changes in legislation, best practice, or emerging risks.

## 18. Contacts

For IT-related enquiries or assistance, users can contact the current IT Services and Support Provider, which can be obtained from the Officers of the Council. If unsure, users can contact the Executive Officer.