

Sandon and Burston Parish Council IT Policy

1. Purpose

This policy outlines the principles and procedures for the use, management, and security of IT systems, devices, and data within Sandon and Burston Parish Council. It aims to ensure that technology is used responsibly, securely, and in compliance with legal and regulatory requirements.

2. Scope

This policy applies to:

- All Parish Council members and employees
- All devices, software, and digital services used for Council business

3. IT Governance

- The Clerk is responsible for day-to-day IT management and liaising with external IT providers.
- The Council will ensure appropriate budget provision for IT maintenance, upgrades, and cybersecurity.
- All IT purchases must be approved by the Council and comply with procurement procedures.

4. Acceptable Use

- Council IT systems and devices must be used only for official Council business.
- Personal use of Council devices is discouraged and must not compromise security or data integrity.
- Users must not install unauthorised software or access inappropriate content.
- All communications via Council email or social media must be professional and in line with Council values.

5. Data Protection and Privacy

- All personal data must be handled in accordance with the UK GDPR and Data Protection Act 2018.
- The Clerk is the designated Data Protection Officer (DPO) and responsible for ensuring compliance and the Council has a Data Protection agreement with Staffordshire County Council .
- Personal data must be stored securely and only accessed by authorised personnel.
- Data breaches must be reported immediately to the Clerk and documented.

6. Email and Communication

- Council members and Clerk email accounts must be used for all official correspondence.
- Emails must be archived and retained in accordance with the Council's Document Retention Policy.
- Councillors are encouraged not use personal email accounts for Council business.
- Clerk emails to Councillors are intended only for the named recipient and may be privileged or confidential, members are reminded not to copy or distribute outside of Council.

- Clerk will have the following in the email signature: The information in this email is intended only for the named recipient and may be privileged or confidential. If you are not the intended recipient, please notify the Clerk immediately and then delete the message and do not copy, distribute or take action based on this email.
- Clerk is responsible for emailing the e-newsletter bi-monthly after the Parish Council meeting to residents who have opted in to receive it. (Database created in March 2026)

7. Website and Social Media

- The Clerk is responsible for maintaining the Council website and ensuring content is accurate and up to date.
- Social media posts are not used by Sandon and Burston Parish Council.

8. Security and Access Control

- Devices must be password-protected and updated regularly.
- Access to sensitive data and systems must be restricted to authorised users.
- Remote access must be secured via VPN or encrypted connections.
- Anti-virus and firewall protection must be maintained on all Council devices.

9. Backups and Disaster Recovery

- Regular backups of Council data must be performed and stored securely.
- A disaster recovery plan must be maintained to ensure continuity of operations in the event of IT failure or data loss.

10. Reporting and Enforcement

- Any IT issues, security concerns, or suspected breaches must be reported to the Clerk immediately.

11. Review and Updates

This policy will be reviewed if required due to changes in legislation, technology, or Council operations.

12. Other Policies to read with this policy

Retention and Disposal of Documents, Risk Management, Freedom of Information and Publication Scheme, Data Privacy Policy.

Date last Ratified/Approved	Version Number	Revision/Amendment Made	New Review date
03.03.2026	1	Policy adopted	May 2026