STAVERTON PARISH COUNCIL
IT and Digital Use Policy

1. Purpose

This policy sets out how councillors, employees, and authorised volunteers of Staverton Parish Council are expected to use information technology (IT) systems and digital data when conducting council business.

It ensures that all digital activity is carried out securely, lawfully, and in accordance with:

- The UK General Data Protection Regulation (UK GDPR);
- The Data Protection Act 2018 (DPA);
- The Freedom of Information Act 2000 (FOI);
- The Smaller Authorities' Proper Practices Guide 2025 (SAPPP), section 1.54; and
- The Web Content Accessibility Guidelines (WCAG) 2.2 AA standards for accessibility.

2. Scope

This policy applies to:

- All councillors, employees, contractors, and volunteers who handle or access council data or systems.
- All devices and software used for council business, including:
    - Council-owned equipment (e.g. laptops, tablets, storage drives); and
    - Personally owned devices (BYOD) when used to access or store council data (e.g. email, documents, or cloud systems).

3. Objectives

The objectives of this policy are to:

1. Protect the Council's digital information from loss, damage, or unauthorised access.
2. Ensure lawful processing and storage of data under UK GDPR and the DPA.
3. Provide clear guidance for all users on the acceptable use of IT and digital systems.
4. Support transparency, accessibility, and the Council's compliance with Assertion 10.

4. Acceptable Use

Users must:

- Use council IT systems and email accounts only for official council business.
- Access and store council data using secure and authorised platforms only.
- Keep devices and files password-protected and encrypted where available.
- Log out or lock devices when unattended.
- Report any loss, theft, or suspected data breach immediately to the Clerk.
- Respect the confidentiality of council information at all times.

Users must not:

- Share passwords or access credentials with unauthorised persons.
- Install unauthorised software on council devices.
- Use personal email accounts for council business (except in exceptional, approved circumstances).
- Copy or store council data on unencrypted removable media (e.g. USB drives).
- Use council systems for personal or political purposes.

5. Personal Device Use (BYOD)

When using personal devices for council business:

- Devices must be protected by a strong password, PIN, or biometric lock.
- Operating systems and software must be kept up to date.

- Access to council email or cloud storage must be through secure channels (e.g. Microsoft 365, Google Workspace, or equivalent with encryption).
- Council data must not be stored locally on personal devices unless necessary and authorised.
- Data must be deleted securely when no longer required for council purposes or upon termination of office/employment.

6. Data Protection and Privacy

All council data must be processed in accordance with the Data Protection Policy and Privacy Notice.

- Personal data must only be collected and processed where necessary for council functions.
- Data must be stored securely and retained only for as long as necessary under the Council's Data Retention and Disposal Schedule.
- Any suspected data breach must be reported to the Clerk immediately, who will assess and record the incident in line with UK GDPR reporting obligations.

7. Email and Communications

- All official correspondence must be conducted via council email accounts.
- Users must verify recipients before sending sensitive information.
- Emails containing personal data should be minimised, and attachments should be password-protected where feasible.
- Spam or suspicious emails must not be opened or forwarded.

8. Website and Accessibility

- The Council will maintain a website compliant with WCAG 2.2 AA accessibility standards.
- Documents published online must be accessible (e.g. properly tagged PDFs or HTML versions).
- The Clerk will ensure the website's Accessibility Statement is accurate and reviewed annually.

9. Cloud Storage and Backups

- Council documents will be stored in a secure, access-controlled cloud environment (e.g. Microsoft OneDrive, SharePoint, or similar).
- Regular backups will be maintained to protect against data loss.
- Access permissions will be limited to authorised personnel only.

10. Security and Incident Management

- Users must report any IT incident, data breach, or suspicious activity to the Clerk immediately.
- The Clerk will maintain an Incident Log and, where applicable, report notifiable data breaches to the Information Commissioner's Office (ICO) within 72 hours.
- Periodic reviews of security controls and procedures will be carried out.

11. Training and Awareness

- The Clerk will ensure all councillors and staff receive annual training on data protection, IT security, and digital compliance.
- New councillors and employees will receive this policy as part of their induction pack.

12. Policy Review and Governance

- This policy will be reviewed annually or sooner if legislation, guidance, or council practices change.
- The Clerk and Responsible Financial Officer will oversee compliance.
- Adoption and amendments will be approved by Full Council and recorded in the minutes.

13. Related Policies and References

This policy should be read in conjunction with:

- Data Protection Policy
- Privacy Notice
- Freedom of Information Policy
- Publication Scheme
- Records Retention and Disposal Policy
- Staff Code of Conduct and Member Code of Conduct

14. Adoption

This IT and Digital Use Policy was approved and adopted by STAVERTON PARISH COUNCIL at its meeting held on MONDAY 16TH MARCH 2026 and will be reviewed annually in line with best practice and the Smaller Authorities' Proper Practices Guide (2025).

Signed:

Councillor Nick Woodall, Chairman of STAVERTON PARISH COUNCIL

Signed:

June Jones, Clerk of STAVERTON PARISH COUNCIL

Adopted at Staverton Parish Council meeting 16th March 2026.

Date of Next Review: March 2027