SALEHURST & ROBERTSBRIDGE
PARISH COUNCIL

Mrs Karen Ripley (Clerk)
The Parish Office
Youth Centre, George Hill
Robertsbridge, East Sussex TN32 5AP

Tel: 01580 882066
Email: clerk@salehurstparishcouncil.gov.uk
Web: salehurstparishcouncil.gov.uk

Information Technology Policy

Adopted: 16 March 2026 Minute Reference: 25/26-69c.i

1. Purpose

This policy defines how IT systems, devices, accounts, and data are used and protected by Salehurst & Robertsbridge Parish Council ("the Council"). It ensures secure, lawful, and efficient handling of council information across council-issued devices, personal devices used for council work, and the council's official *.gov.uk* website. Council information / data may be:

- General Council Data – non-personal, operational information, such as policies, reports, minutes and any information already in the public domain.
- Personal – information relating to an identified or identifiable living person, such as names, addresses or other personal information.

---

2. Scope

This policy applies to:

- The **Clerk** and **Assistant Clerk**, who use council-issued laptops and *Microsoft 365 Business Standard licences.*
- The **nine Councillors**, who use personal devices with *Microsoft 365 Business Basic* licences.
- All council-owned accounts, systems, and data, including the *.gov.uk* email domain and the official *.gov.uk* parish council website.
- Any personal device used to access council information.

---

3. Roles and Responsibilities

3.1 **Clerk**

- Manages day-to-day IT operations and acts as the primary contact for the website provider and IT support contractor.
- Ensures compliance with this policy and relevant legislation.
- Oversees user accounts, permissions, and access to council systems.

- Ensures a regular offsite backup system is in place for the two *Microsoft 365 Business Standard* accounts.
- Ensures suitable anti-virus software is installed on council issued laptops.
- Reports data breaches to the Chair and the ICO where required.

3.2 **Assistant Clerk**

- Supports the Clerk in managing IT systems and the council website.
- Follows all security and data handling requirements.

3.3 **Councillors**

- Use council email accounts for *all* council business.
- Protect council information accessed on personal devices.
- Report any suspected data breach or device loss immediately to the Clerk.

---

4. Devices and Equipment

4.1 **Council-Issued Devices (Clerk & Assistant Clerk)**

- Laptops remain council property and must be used primarily for council business.
- Devices must be protected with strong passwords, automatic screen locks, and up-to-date security patches.
- Devices must not be shared with family members or third parties.
- Devices must be locked when the user leaves the work station for any reason.

4.2 **Personal Devices (Councillors)**

- Councillors may use personal devices to access M365 and email.
- Devices must have screen locks, security updates, and antivirus protection.
- Council data must not be stored on personal devices unless absolutely necessary and approved by the Clerk.

---

5. Accounts, Passwords, and Authentication

5.1 **Microsoft 365 Accounts**

- All staff and councillors are issued a *.gov.uk* email address.
- Accounts must *only* be used for council business.
- Access is removed when a councillor or staff member leaves the council.

5.2 **Password Requirements**

- The Clerk and Asst. Clerk will use a password management system approved by the Clerk.
- Strong passwords with a minimum 12 characters.
- Must not be reused from or for other accounts.
- Must not be shared.

5.3 **Multi-Factor Authentication (MFA)**

- MFA is *mandatory* for all users.
- Personal mobile phones may be used for MFA.
- Backup authentication methods should be configured where possible.

---

6. Data Storage and Management

6.1 **Approved Storage**

- Microsoft OneDrive and SharePoint (council accounts only).
- The Clerk and Assistant Clerk may use encrypted USB devices provided by the Council and approved by the Clerk. And their Council issued laptops, where necessary for Council Business (e.g. off-site working where documents will be required when there is no internet access or for limited drafting purposes).
- The council's website content management system (CMS) for public documents.

6.2 **Prohibited Storage**

- Personal cloud services (e.g., Dropbox, Google Drive, iCloud).
- Personal email accounts.
- Unencrypted USB devices.
- No personal or sensitive data / databases should be kept by Councillors on any storage media e.g. CD's, DVD's, USB's, laptops or personal home-based computers.

6.3 **Data Retention**

- The council follows its adopted Data Retention Policy.
- Users must not delete council records unless authorised.

---

7. Email and Communication

- All council business *must be* conducted using *.gov.uk* email accounts.
- Personal email accounts *must not* be used for council work.
- Council email accounts *must not* be used for personal emails.

- Sensitive information must not be sent unencrypted.
- Forwarding emails from Councillor email addresses is not permitted, even to the Councillor's own, personal email address.
- Users must remain alert to phishing and report suspicious messages.
- The Council may monitor email activity, so that compliance with this policy and other relevant policies and regulations can be effectively managed.

---

8. Remote Working

8.1 **Staff Working from Home**

- Clerk and Assistant Clerk may work from home using council laptops.
- Home Wi-Fi must be password-protected.
- Work must not be carried out on personal devices unless authorised.

8.2 **Councillors Working from Home**

- Councillors may access M365 via personal devices.
- Confidential documents / personal data must not be downloaded to personal devices.

---

9. Software and Updates

- Only approved software may be installed on council laptops.
- Automatic updates must be enabled.
- Users must not bypass security settings or install unauthorised applications.

---

10. Information Security

10.1 **Data Breaches**

A data breach includes:

- Loss or theft of a device.
- Unauthorised access to council accounts.
- Accidental sharing of personal data.

All breaches must be reported to the Clerk immediately.

10.2 **Malware and Threats**

Users must:

- Not open suspicious attachments or links.
- Report unusual device behaviour.
- Avoid public Wi-Fi for council work unless using a secure VPN.

---

11. Councillor Leavers and Starters

11.1 **Starters**

New councillors receive:

- M365 Business Basic licence.
- *.gov.uk* email address.
- Access to relevant SharePoint/Teams areas.

11.2 **Leavers**

- Accounts are disabled within 24 hours.
- Access to SharePoint and Teams is removed.
- Any council data stored on personal devices must be deleted.

---

12. Acceptable Use

Users must:

- Use IT systems responsibly and lawfully.
- Not use council systems for political campaigning.
- Not store or transmit offensive, discriminatory, or illegal content.
- Not use council accounts for personal business.

---

13. Council Website Management

13.1 **Website Hosting and Support**

- The council's *.gov.uk* website is provided, hosted, and supported by an external company specialising in compliant websites for local authorities.
- The provider is responsible for:
    - Server security and maintenance.
    - Website availability and uptime.
    - Technical support and updates.

- Ensuring the platform itself meets accessibility requirements.

13.2 **Clerk and Assistant Clerk Responsibilities**

- Manage day-to-day website content, including:
  - Agendas, minutes, policies, and statutory documents.
  - News updates and public notices.
  - Councillor information and contact details.
- Ensure published documents meet accessibility requirements (e.g., readable PDFs, appropriate alternative text on images).
- Ensure personal data is not published unless legally required or explicitly authorised.
- Maintain secure login credentials for the website CMS.
- Report any website issues or suspected security concerns to the provider promptly.

13.3 **Website Security**

- Only authorised staff may access the website CMS.
- Passwords must meet council password standards.
- MFA must be used where supported.
- Website content must not be uploaded from untrusted or unknown sources.

13.4 **Compliance**

The website must comply with:

- Web Content Accessibility Guidelines 2.2 AA and the Public Sector Bodies (Websites and Mobile Applications) (No. 2) Accessibility Regulations 2018.
- General Data Protection Regulations (GDPR) 2016 and the Data Protection Act (DPA) 2018.

---

14. Monitoring and Audit

- The council may audit access logs, email usage, and data storage for compliance.
- Monitoring will be proportionate and lawful.

---

15. Policy Review

This policy will be reviewed annually or sooner if:

- Technology changes.
- Legislation changes.