Information Technology (IT) Policy

1. Introduction

Stapeley & District Parish Council recognises the importance of secure and effective use of information technology (IT) in supporting its work, operations, and communications. This policy sets out how IT resources are to be used, managed, and safeguarded to ensure compliance with statutory responsibilities, including Assertion 10 of the Annual Governance and Accountability Return (AGAR) as referenced in the 2025–26 SAAP guidance.

This policy complements the Council's adopted Email Communications Policy and adopted Social Media Policy, which must be complied with at all times.

---

2. Scope

This policy applies to:

- The Clerk (the Council's only employee provided with IT equipment),
- All councillors, who operate on a Bring Your Own Device (BYOD) basis,
- Any contractors, volunteers, or third parties who are given access to council information.

It covers the use of laptops, mobile phones, networks, cloud storage, and personal devices where these are used for council business.

---

3. Equipment and Software

- The Clerk is issued with a Council-owned laptop and mobile phone, both backed up using secure cloud-based services (OneDrive).
- Councillors are not issued with IT equipment and are responsible for ensuring their own devices meet the requirements of this policy.
- Installation of unauthorised software on Council-owned devices is prohibited.
- All software must be kept updated with security patches applied promptly.

---

4. Passwords and Access Control

- Passwords must be at least 10 characters long and contain a mix of upper and lower case letters, numbers, and symbol or formed of 3 words plus 1 symbol and 1 number.
- Passwords must never be shared.
- Devices used for council business must be protected with a login password, PIN, or biometric security.
- Where councillors share a personal device with family members, they must ensure that council information is stored in a way that is inaccessible to others.

---

5. Data Storage and Handling

- Official Council documents should be stored in the Council's cloud-based systems or on the Clerk's council-issued laptop.
- Councillors may download shared documents for reference but should delete them once they are no longer required.

- Highly sensitive information will only be shared as view-only through secure cloud storage or provided in paper format at meetings.
- Documents containing personal data must not be stored on personal devices when no longer required.

---

6. Use of Devices and Internet

- IT resources are to be used for official Council purposes. Limited personal use by the Clerk on Council-owned devices is permitted provided it does not interfere with duties.
- BYOD councillors must use their devices responsibly and ensure anti-virus software and operating systems are up to date.
- Council business must not be conducted through insecure platforms or messaging services.
- WhatsApp groups may be used for informal sharing of information only and must not be used for decision-making.
- The Council's adopted Email Communications Policy and Social Media Policy apply at all times when councillors or staff are acting in a council capacity.

---

7. Security and Backups

- The Clerk's devices are automatically backed up to OneDrive.
- Councillors must take reasonable steps to safeguard any temporary copies of documents saved on personal devices, including using secure deletion when no longer required.
- Lost or stolen devices used for Council business must be reported immediately to the Clerk and steps taken to revoke access to council accounts where applicable.

---

8. Confidentiality and Data Protection

- Users must comply with data protection legislation, including GDPR, in handling personal information.
- Personal data should only be collected, used, and stored where necessary and must be protected from unauthorised access.
- Data must not be disclosed to third parties without proper authority.

---

9. Misuse and Breach of Policy

Examples of misuse include, but are not limited to:

- Using Council devices or information for personal gain,
- Attempting to bypass or disable security measures,
- Sharing confidential data inappropriately,
- Allowing non-council members to access restricted information.

Breaches of this policy may result in disciplinary action for staff and referral to the Monitoring Officer for councillors.

---

10. Training and Awareness

- The Clerk will keep informed of best practice in IT security.
- Where appropriate, councillors will be provided with guidance on secure handling of documents and safe online practices.

---

11. Policy Review

This policy will be reviewed annually to ensure it remains relevant and compliant with legislation.

This policy was adopted by the Council at the meeting held on the 17th Nov 2025