SEATON ROSS PARISH COUNCIL

Information Technology (IT) Policy

1. Introduction

The purpose of this policy is to ensure that all employees, councillors, and third parties using Seaton Ross Parish Council information technology (IT) understand what is and is not permitted. The policy supports the appropriate use of Council equipment, safeguards the security of IT systems and data, and assists compliance with relevant legislation.

2. Definitions

- **Users** — councillors, employees, and third parties acting on behalf of the Council.
- **Data** — digitally stored information including, but not limited to, documents, copyrighted or copyrightable text, images, personal information, and accounting information.
- **IT hardware/software** — includes computers, internet access, remote access connections, email servers, file storage, webmail, smartphones, telephones, websites, mobile phones, and related systems.

3. Scope

This policy applies to all councillors, employees, and third parties acting on behalf of the Council, including contractors. It covers the use, management, and safekeeping of IT hardware, software, and data.

4. IT Provision

All devices, software, data access, and services provided remain the property of the Council and must be recorded on the asset register. At the end of any period of office, employment, or contracted work, all equipment must be returned to the Clerk, Chair, or Vice-Chair in full working condition. Replacement or repair costs may be charged if equipment is lost, damaged, or not returned within 14 days.

Users must comply with all relevant Council policies, procedures, and UK legislation relating to IT use.

4.1 Principles for IT Provision

All IT provision should:

- demonstrate value for public money;
- support efficient working and avoid unnecessary waste;
- consider cost versus time savings achievable through technology;
- maintain the privacy of councillors, employees, subcontractors, and parishioners;
- align with other Council policies, including the Environmental Vision Statement & Strategy.

A review of IT requirements must be undertaken at least every four years (aligned with council elections) or within three months of new staff appointments.

Council-provided hardware must be used solely for Council business.

The Parish Council WhatsApp group is for **notifications only**. No Council business may be transacted via WhatsApp, especially when accessed on personal devices.

5. Privacy and Data Protection

Users must:

- not leave accounts logged in on unattended or unlocked devices;
- use secure methods for storing and accessing data;
- refrain from making unauthorised changes to IT systems or information;
- avoid accessing data or software they are not authorised to use;
- not transfer Council data or software to external parties without proper authority;
- comply with the General Data Protection Regulation Policy and Document Retention Policy;
- comply with all relevant legislation relating to IT software.

Users accessing Council systems or data on personal devices are responsible for ensuring compliance with this policy and all data protection requirements.

5.1 Email Use

- All councillors and employees will be provided with a Council email address.
- This must be used for all Council-related correspondence.
- Emails must include an appropriate footer and GDPR disclaimer.
- External emails must be professional in tone.
- Councillors who choose not to use their Council email address do so at their own risk; the Clerk is not responsible for missed information.

Personal use of Council-provided communication services, software, or data is not permitted unless the data is already publicly available.

Correspondence undertaken on behalf of the Council—whether on Council or personal devices—must be provided to the Clerk or Chair upon request, particularly in relation to Freedom of Information requests.

Users must note that during an ICO investigation, equipment (including personal devices) may be seized for the duration of the investigation.

6. Passwords and Access Control

- The Clerk will set passwords for Council-owned email accounts. These must not be changed, as the Clerk requires access for account closure.
- Where available, two-factor authentication must be enabled, preferably using a hardware security key or secure authentication app.

- Devices provided for extended use should have biometric authentication enabled under a Council-managed account.

7. Risk Management

The Council maintains insurance for all IT equipment.

Users must take reasonable steps to prevent theft or unauthorised use. Equipment must not be left in unattended vehicles unless unavoidable and must be stored out of sight if so.

Any loss or damage must be reported immediately to the Clerk and Chair. Criminal damage will be reported to the Police.

Any loss of personal data resulting from equipment loss or theft must be reported to the Clerk, Chair, and the Information Commissioner's Office (ICO).

An annual risk assessment must be conducted covering IT hardware, software, and stored data.

8. Application of the Policy

Failure to comply with this policy may result in disciplinary action.
