Stalmine-with-Staynall Parish Council Information Technology (I.T) Policy

Introduction

Stalmine-with-Staynall Parish Council recognises the importance of effective and secure information technology (IT) and email usage in supporting its business, operations, and communications.
The Council understands that it has a duty to ensure the proper security and privacy of its computer systems and data. All users have some responsibility for protecting these assets.
The Clerk is responsible for the implementation and monitoring of this policy.
This policy outlines the guidelines and responsibilities for the appropriate use of IT resources and email by council members, employees, volunteers, and IT contractors.

Definitions

Users – councillors, employees and third parties acting on behalf of the Council.
Data – digitally stored information including (but not limited to) documents, copyrighted / copyrightable text, images, personal information, accounting information.
IT hardware/software – includes, but is not limited to computers, internet access, remote access connections, email servers, file storage, webmail, smart phones, telephones, website, mobile phones etc.

Scope

This policy covers the use of IT, both hardware and software, for all councillors, employees and third parties acting on behalf of the Council (Users), and contractors, management and safekeeping of data.

Acceptable use of IT resources and email

Stalmine-with-Staynall Parish Council IT resources and email accounts are to be used for official council-related activities and tasks. All users must adhere to ethical standards, respect copyright and intellectual property rights, and avoid accessing inappropriate or offensive content.

IT provision

The device, software, data access and services provided remain property of the Council and shall be recorded on the asset register.
Users must comply with all relevant policies, procedures and UK legislation with respect to the use of IT hardware.

All IT provision should:

- demonstrate value for use of Council money;
- provide value for Council or clerk use, whilst enabling efficient working and not contributing to secondary waste;
- include consideration of cost vs time spent carrying out tasks which could be offset by the use of technology;
- maintain privacy of councillors, Council employees, subcontractors and parishioners;
- adhere to other policies as much as is possible
- have regular back-ups with an external drive (clerks laptop)

A review of the Council's IT requirement should be conducted at least every four years, when council elections take place and new councillors take office, or within three months of new members of staff starting with the Council.
Hardware provided should only be used for Council business and not personal use

Device and software usage

Where possible, authorised devices, software, and applications will be provided by Stalmine-with-Staynall Parish Council for work-related tasks. Unauthorised installation of software on authorised devices, including personal software, is strictly prohibited due to security concerns.

General Principles
All employees, members and other users should be aware of the increasingly sophisticated scams and risks posed to cybersecurity and when in any doubt should seek guidance from the Town Clerk. As a general rule, users will never be asked to share passwords by email and users should be aware of odd language used in emails which may indicate a fraudulent email.

All employees, members and other users of council IT equipment must be familiar with and abide by the regulations set out in the council's 'Data Protection & Retention Policy'.

All council devices will have up-to-date antivirus software installed and this must not be switched off for any reason without the authorisation of the Clerk.

All users are reminded that deliberate unauthorised use, alteration, or interference with computer systems, software or data is a breach of this policy and in some circumstances may be a criminal offence under the Computer Misuse Act 1990.

All software installed on council devices must be fully licensed and no software should be installed without authorisation from the Clerk.

Privacy and data protection
Users must:

- not leave their user accounts logged in on an unattended and unlocked device;
- use suitability secure methods for storing and accessing data and services;
- not perform any unauthorised changes to the IT systems or information; changes must only be made with agreement from the Chair and at least one other councillor, or at full Council where applicable;
- not attempt to access or use data or software that they are not authorised to use or access;
- not give or transfer Council data or software to any person or organisation outside the Council without the appropriate authority and reason to do so;
- adhere to the Data Protection Policy and Document Retention Policy;
- comply with all relevant policies, procedures and UK legislation with respect to the use of IT software; if unsure about this then users should check with the Clerk or Chair.

Where users use their own hardware to access Council systems or data, they are responsible for ensuring the security of systems and data as per this policy, the Data Protection Policy and the Document Retention Policy.
An email address will be provided to all councillors and Council employees and should be the only address used for official or unofficial Council correspondence.
Personal use is not permitted for any Council provided communication services, software applications (downloaded or software as a service) or data, unless such data is already in the public domain.
Any correspondence undertaken on behalf of the Council on Council provided or personal devices or services, where retained in line with the Retention Policy, should be provided upon request to the Clerk or Chair, particularly, but not limited to the case of a Freedom of Information request.

Passwords and access to systems and services
Passwords should be either a minimum of 20 random letters, numbers or symbols (ideally 25 plus), or four or five random words joined with non-alphanumeric characters.

Where a service offers two factor authentication then this must be used, if possible, with a hardware security key or software two factor authentication (e.g. google authenticator) secured by a strong log-in or password.

Where a device is provided for a reasonable period of time to a Councillor or employee of the Council and this device offers biometric authentication, then this should be activated under a Council managed account.

Risk Management
As part of its risk management the Council maintains insurance on the equipment provided.
All equipment must be secured from theft or unauthorised use as far as is practical.
When travelling with equipment, it should not be left in an unattended vehicle unless there is no other option, in which case it should be secured out of sight.
Any loss of, or damage to equipment should be reported as soon as possible to the Clerk and Chair and any criminal damage will be reported to the Police by the Clerk.
Any loss of personal data as the result of loss or theft of equipment shall be reported to the Clerk and Chair and Information Commissioner's Office (ICO).
An annual risk assessment should be undertaken regarding use and security of Council IT hardware, software and stored data.

Misuse of IT
IT systems will be monitored for misuse and all misuse is prohibited.
Misuse includes, but is not limited to:

- Creation or transmission of any offensive, obscene or indecent images, data or other material or any data capable of being resolved into obscene or indecent images or material
- Creation of material which is designed or likely to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission of defamatory material
- Transmission of material which in anyway infringes the copyright of another person
- Transmission of unsolicited commercial advertising material to networks belonging to other organisations
- Deliberate actions or activities with any of the following characteristics:
- Wasting staff effort or networked resources
- Corrupting or destroying other users' data
- Violating the privacy of other users
- Disrupting the work of other users
- other misuse of the networked resources by the deliberate introduction of viruses/malware
- Playing games during working hours
- Altering the set up or operating perimeters of any computer equipment without authority.
- Unauthorised access, use, destruction, modification and/or distribution of council information, systems or data is prohibited

Application of the Policy
Not adhering to the terms set out in this policy may result in disciplinary proceedings.

Document control			
Document tile	I.T Policy		
Version number	Date approved	Author	Next Review
V1.0	July 2025	Debbie Smith	July 2026