The Vestry Rooms
25 Fore Street
St Erth TR27 6HT
Tel: 01736 757575
Email: clerk@sterth-pc.gov.uk
Website: www.sterth-pc.gov.uk

Information Technology Policy

Introduction

The purpose of this policy is to ensure that all employees, councillors and any third parties using St Erth Parish Council information technology (IT) have a clear understanding of what is and is not permitted. This will ensure the appropriate use of the Council's equipment, safeguard the security of its IT systems and data, and assist compliance with any relevant legislation.

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.

IT provision

The device, software, data access and services provided remain property of the Council and shall be recorded on the asset register. At the end of any period of holding office, employment with or work for the Council, all equipment must be returned to the Clerk, Chair or Vice-Chair in full working condition. If equipment has been lost or damaged, a charge may be made for its replacement or repair.

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, particularly the Environmental Vision Statement & Strategy.

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.

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.

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 & Chair and any criminal damage should 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 & 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.

Application of the Policy

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

Adopted	4th April 2023	207/04/22-23a)
Review due	April 2024 then 2 yearly	