Saltash Town Council

Policy/Procedure: **Provision Of It And Acceptable It Usage DRAFT**

Date of Adoption:

This is a Policy or Procedure document of Saltash Town Council to be followed by both Councillors and employees.

Current Status			
Version	1 NEW	**Approved by**	
Date	March 2021	**Date of approval**	
Responsible Officer	AJT	**Minute reference**	
Responsible Committee	P&F	**Review date**	Four yearly or if required

Version History			
Date	**Version**	**Author/Editor**	**Comments**
March 2021	1	AJT	New policy

Review Record				
Date	**Type of Review**	**Minute number**	**Summary of actions**	**Completed by**

Document Retention	
Document retention period	Until superseded

SALTASH TOWN COUNCIL

PROVISION OF IT AND ACCEPTABLE IT USAGE POLICY

This policy should be read in conjunction with the following:

Information and Data Protection Policy
Management of Transferable Data Policy
GDPR 2018
Data Protection Act 2018
Computer Misuse Act 1990
Members of staff should also refer to the Employee Handbook
Equality and Diversity Policy

Context:

Saltash Town Council provides IT equipment to both staff and councillors to enable them to carry out their duties effectively in Council buildings and when working from home or in the community. This policy is in two parts – the provision of IT equipment and the individual's responsibilities when using IT.

Scope:

This policy sets out the correct, appropriate and expected use of Saltash Town Council computing and networking facilities to ensure safe and reliable operation. This extends to all IT facilities including software, hardware, staff computers, Councillors devices, telephones (mobile and internal) provided and maintained by Saltash Town Council.

Part 1

Provision of IT Equipment

Virus detection is installed and managed centrally by the IT Consultant. Individuals must not remove or disable anti-virus software or attempt to remove virus infected files. These should be referred to the IT Consultant.

a. Employees

All employees are issued with appropriate IT equipment on commencement of employment with the Town Council. This may include a laptop, mobile phone, use of a computer in a council building, memory devices (e.g. USB) according to the requirements of the role. A unique email account, user ID and password are also issued with an authentication device if appropriate. Access levels to systems and information will be authorised appropriate to the users' job role.

Upon termination of contract all Council owned property should be returned. The Line Manager will ensure all authorised access is promptly removed.

b. Councillors

On joining the Council Members will be offered a device (usually a tablet or laptop) running a supported operating system, with the capability for joining

virtual meetings and accessing council emails and information, on long term loan for the length of their tenure as Town Councillor. The device will be procured by the Town Council and will be preloaded with software which will be licensed and managed by the Town Council IT Consultants. The specification of the device will ensure that it remains fit for purpose for the four-year term of the Council.

The Town Council will provide all Councillors with a unique email address, user ID and password with access to selected areas of the IT system.

On cessation of service as a Town Councillor the tablet/laptop/device should immediately be returned to the Town Council and all access rights will be rescinded.

c. Loss/Damage

i. Employees

Employees have a responsibility to take reasonable care of any device they are allocated, particularly when taking off site. Any loss or damage should be immediately reported to their Line Manager.

ii. Councillors

The Town Council will insure devices loaned to Councillors. It is accepted that these devices will be taken off site and Councillors have a responsibility to take reasonable care of the device. Any loss or damage should be immediately reported to the Assistant Town Clerk. Where a device has to be sent for repair it may be possible to provide a loan device but this cannot be guaranteed.

At the end of life of the devices it will be securely wiped of all data and donated to a suitable organisation for distribution to children/young people without access to IT for home study.

Part 2

Acceptable IT usage and user responsibilities

a. All authorised users of Saltash Town Council computing facilities and network must ensure that:

- Any breaches or suspected security incidents concerning the Town Council network or computing facilities must be reported immediately.[1]
- Passwords, PINs or any other unique authentication credentials should not be disclosed to anyone under any circumstances.

[1] Data breaches – Senior Policy & Data Compliance Monitoring Officer
Security breaches – IT Consultant + Assistant Town Clerk

- Passwords, PINs or any other unique authentication credentials should not be written down anywhere.
- You should change your password immediately if you believe it may have been compromised.
- Always ‘screen lock’ any device when leaving it unattended.
- Never attempt to perform any unauthorised changes to STC IT systems.
- All data held on STC systems may be subject to Freedom of Information or Subject Access Requests. For this reason, personal use of STC computing and network facilities cannot be deemed to be private.
- Do not use or attempt to use another individual’s account.
- Never exceed the limits of your authorisation or specific business need by attempting to access systems or information that you do not need in order to carry out your role. A deliberate and intentional attempt to access unauthorised resources breaches the Computer Misuse Act 1990.
- If you believe you have mistakenly been granted access to IT systems, information or resources which are not appropriate or authorised by you, this should be immediately reported as a possible incident. Under no circumstances should you attempt to further access the information/resources.
- Do not facilitate or attempt to facilitate access for anyone who is not authorised to access specific information or systems.
- Never copy, store or transfer data or software owned by STC to any unmanaged device without the explicit written consent of the asset owner.
- Your login ID identifies you as an individual and holds you directly accountable for all actions which take place under your credentials. A logged in session should not be shared with anyone else.

b. Working off site

- Equipment and media taken off site must not be left unattended in public places and not left in sight in a car.
- Information must be protected against loss or compromise when working remotely.
- Particular care should be taken with the use of mobile devices such as mobile phones, laptops and tables.

c. Internet and Email Conditions of Use

Use of STC internet and email is intended for business use. Personal use is not permitted and all individuals are accountable for their actions on the internet and email systems.

Emails must not be opened on a non STC device. Any employee who opens STC emails or data on a personal device unless they have prior and exceptional written permission from their line manager may be subject to disciplinary action.

Individuals must not:

- Use the internet or email for purposes of harassment or abuse.
- Use profanity, obscenities or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which STC considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the emails systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to STC, alter any information about it, or express any opinion about STC, unless they are specifically authorised to do this.
- Send unprotected sensitive or confidential information externally.
- Forward STC mail to personal (non-STC) email accounts.
- Make official commitments through the internet or email on behalf of STC unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Consultant.