Policy Group:
Employees/Members

APPENDIX C

IT POLICY

RESPONSIBLE COMMITTEE: POLICY & FINANCE

This is a policy/procedure document of Saltash Town Council to be followed by both Town Councillors and Employees.

Current Document Status			
Version	2026	**Approved by**	
Date		**Responsible Officer**	
Minute no.		**Next review date**	Annual or as required

Version History					
Date	**Version**	**Author/ editor**	**Committee/ date**	**Minute no.**	**Notes**
02/2026	1	ELS			New policy/Merged Policy Refers to the following policies: - Social Media - Communications Policy & Strategy - Employee Handbook - Data Protection and Retention

Document Retention Period
Until superseded

IT Policy

Introduction:

Saltash Town Council provides IT equipment to both staff and Town Councillors to enable them to carry out their duties effectively in Town 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.

Purpose:

The purpose of this IT Policy is to establish clear expectations for how Saltash Town Council’s IT equipment, systems and digital resources are to be used by Councillors, staff and other authorised users in the course of their duties. The policy aims to ensure that all users understand their responsibilities when accessing or handling council-provided technology, whether on council premises, at home or in the community.

Scope:

This policy sets out the correct, appropriate and expected use and care 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, Town Councillors devices, telephones (mobile and internal) provided and maintained by Saltash Town Council.

This policy supports compliance with Assertion 10 of the Annual Governance and Accountability Return (AGAR), ensuring the Town Council manages digital systems, data, cybersecurity, email, and website accessibility in accordance with statutory requirements.

1. Computer Use and Equipment

Saltash Town Council provides appropriate IT equipment to employees when they begin their employment, and to Town Councillors upon joining the Town Council. Equipment may include laptops, mobile phones, office computers, or memory devices, depending on the requirements of the role. Councillors are offered a council-owned device for business use only, loaned for the duration of their tenure and capable of accessing council emails, information and virtual meetings.

All devices are procured by the Town Council and licensed and managed by the Town Councils IT consultant. Devices are specified to remain fit for purpose throughout their expected period of use.

Employees and Town Councillors use an authority-owned email domain for all official correspondence. Each user is assigned a unique ID and password, with system access permissions configured according to their role, responsibilities, and authorised areas of the IT system.

Upon termination of an Employees contract or Cessation of Service as a Town Councillor, all Town Council owned IT equipment must be returned immediately, and all associated access rights will be removed.

1.1 Hardware

1.1.1 Saltash council computer devices and equipment are provided for council purposes only. Devices must not be shared with other family members or loaned to other individuals.

1.1.2 Locking computers when leaving desk, all councillors, staff, and other authorised users must lock their computers when leaving their desks to prevent unauthorised access. This applies to all council and personal devices used for work. Failure to comply may lead to disciplinary action.

1.1.3 All computer and other electronic equipment supplied should be treated with good care at all times. Computer equipment is expensive, and any damage sustained to any equipment will have a financial impact on the council.

1.1.4 Computer and electronic hardware should be kept clean, and every precaution taken to prevent food and drink being dropped or spilled onto it.

1.1.5 Any faults or necessary repairs must be reported to the Town Clerk and the Town Council IT Consultant.

1.2 Portable Devices

1.2.1 Portable equipment includes laptops, mobile and smart phones with email capability and access to the internet.

1.2.2 Council back up procedures specific to portable equipment should be followed at all times. Information must be protected against loss or compromise when working remotely.

1.2.3 All portable equipment should be stored safely and securely when not in use in the office. They should not be left unattended in public places and not left in sight in a car.

1.2.4 Employees that work remotely must enable a two-factor authentication application (Duo Mobile) on their Town Council/Personal Mobile to access a secure connection when working remotely. Any associated cost is covered by the employer not the employee.

1.2.5 Saltash Town Council has adopted the use of a Mobile Device management (MDM) System to streamline the usage of Town Council issued mobile devices to protect the data of the user and the Town Council. Employees issued with a work phone should ensure it is always switched on during work hours.

1.3 Responsibility for Loss or Damaged Equipment

1.3.1 Employee Responsibility:

- Employees are expected to take reasonable care of the equipment assigned to them.
- Any loss or damage to Town Council equipment must be reported immediately to the Line Manager.
- At the end of the device's lifecycle, all data will be securely erased, and the device will be recycled.
- Employees will be responsible for the repair / replacement of Town Council equipment if the damage or loss is due to negligence, misuse, or failure to follow proper handling and maintenance guidelines.

- In the event of loss or damage Saltash Town Council reserves the right to cover only part or none of the costs for damage or repairs. Please refer to **Appendix B** for the process for reporting loss or damage.

1.3.1 Town Councillor Responsibility:

- Town Councillors are expected to take reasonable care of the equipment assigned to them.
- Any loss or damage to Saltash Town Council equipment must be reported immediately to the Town Clerk or in their absence the Office Manager / Assistant to the Town Clerk.
- At the end of the device's lifecycle, all data will be securely erased, and the device will be recycled.
- Town Councillors will be responsible for repair or replacement costs if the damage or loss is due to negligence, misuse, or failure to follow proper handling and maintenance guidelines.
- In the event of loss or damage Saltash Town Council reserves the right to cover only part or none of the costs for damage or repairs. Please refer to **Appendix B** for the process for reporting loss or damage.

1.3.2 Consequences for Non-Compliance:

- Employees who fail to report damage, misuse, or loss of equipment in a timely manner may be subject to disciplinary action.
- In cases of repeated negligence or intentional damage, Saltash Town Council may seek to recover the costs of repair or replacement.

2. Health and Safety

2.1 Councillors, staff and other authorised users who work in council offices will be provided with an appropriate workstation and undertake regular DSE reviews to ensure

2.2 The council has a duty to ensure that regular appropriate eye tests, carried out by a competent person, are offered to employees using display screen equipment. Further details are set out in the councils Employee Handbook.

2.3 Any VDU user who feels that their workstation requires changes to make it compliant must speak to their line manager.

2.4 If any hazards are detected at a workstation, including 'noises' from the IT equipment, this should be reported immediately to the IT Consultant.

3. Internet, Teams and Official Email Protocol

3.1 Internet, Teams and Email Conditions of Use

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

Individuals must not:

- Use the internet, Teams 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, Teams 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.
- All users must use the council's generic functional email accounts where applicable.

- Personal email accounts must never be used for council business under any circumstances.
- 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, Teams 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.

3.2 Official Email Protocol

3.2.1 Employees: 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.

3.2.2 Personal email accounts must not be accessed on Council-owned devices, nor used for conducting any Town Council business.

3.2.3 Town Council email facilities are intended to promote effective and speedy communication on work-related matters. Although we encourage the use of email, it can be risky.

3.2.4 Councillors, staff, and other authorised users need to be careful not to introduce viruses onto council systems and should take proper account of the security advice.

3.2.5 On occasion, it will be quicker to action an issue by telephone or face to face, rather than via protracted email chains. Emails should not be used as a substitute for face to face or telephone conversations. Councillors, staff, and other authorised users are expected to decide which is the optimum channel of communication to complete their tasks quickly and effectively.

3.2.6 These rules are designed to minimise the legal risks run when using email at work and to guide councillors, staff, and other authorised users as to what may and may not be done. If there is something which is not covered in the policy, councillors, staff, and other authorised users should ask Saltash Town Councils IT Consultant rather than assuming they know the right answer.

3.2.7 All councillors, staff, and other authorised users who need to use email as part of their role will be given their own council email address and account. The council may, at any time, withdraw email access, should it feel that this is no longer necessary for the role or that the system is being abused.

3.2.8 Email messages sent on the council's account are for council use only. Personal use is not permitted.

3.2.9 All email use must comply with relevant legislation including data protection (UK GDPR), computer misuse laws and council policies

3.2.10 Email communications cannot be guaranteed as private. The Town Council reserves the right to access, intercept or monitor email usage at any time to ensure compliance with policy, data protection and security requirements.

4. Website Standards and Accessibility (WCAG 2.2)

4.1 Saltash Town Council is committed to providing a website that is accessible, in accordance with the Public Sector Bodies (Website and Mobile Applications) (No.2) Accessibility Regulations 2018.

4.2 While Saltash Town Council is not yet able to meet all accessibility requirements for its website, compliance will be achieved from 2026. In the meantime, where an accessible version of a document is required, members of the public are asked to contact the Council office so that an accessible format can be provided.

4.3 The Town Council will maintain an up-to-date Accessibility Statement as required by law.

4.4 The Town Council recognises that the website is currently partially compliant with WCAG 2.2 AA Standard and shall take reasonable and proportionate measures to achieve and maintain compliance.

4.5 The Town Council shall work to ensure that it’s website is accessible from multiple devices and formats, including desktop, mobile and text-only formats.

4.6 Accessibility shall be considered when implementing website changes, upgrades, new functionality and content.

4.7 The website shall support user adjustment of font size, colour contrast, and display settings using standard browser and device functionality.

4.8 The Town Council shall provide information and documents in alternative accessible formats upon request to the Town Clerk.

4.9 The Town Council shall periodically review website accessibility and identify areas for improvement.

4.10 Users shall be able to report accessibility issues by contacting the Town Council Office.

4.11 Accessibility compliance is subject to oversight by the Equality and Human Rights Commission (EHRC).

4.12 The Town Council will ensure all legally required information is published on its website, including FOI publications and Transparency Code items.

5. Cybersecurity Basics

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 immediately referred to the IT Consultant via the helpdesk.

5.1 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.
- Passwords, PINs or any other unique authentication credentials should not be disclosed to anyone under any circumstances.
- 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.
- All users must complete regular cybersecurity awareness training.
- The Council shall periodically review cyber security arrangements and implement improvements where reasonably practicable.
- All councillors and staff must complete periodic data protection and cybersecurity training.

6. Social Media Use and Boundaries

Refer to Saltash Town Councils Social Media Policy and Communications Policy and Strategy.

7. Data Protection, Retention, Storage and GDPR Compliance

Refer to Saltash Town Councils Data Protection and Retention Policies.

7.1 Legal Compliance – All personal data must be processed in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

7.2 Secure Storage – Personal and confidential data must be stored securely, with access restricted to authorised personnel only, granted on a need-to-know basis.

7.3 Security Measures – Systems must use strong passwords, multi-factor authentication where available, up to date software, anti-malware protection, and secure, regularly tested backups.

7.4 Secure Handling – Sensitive or confidential data must be transmitted and shared using approved methods and securely destroyed when no longer needed.

7.5 Data Retention – Data must be retained according to Saltash Town Councils Data Protection and Retention Policy and securely deleted when no longer required.

8. Remote Working

Refer to 1.2 Portable Devices, 3.2 Official Email Protocol and the Employee Handbook.

9. Monitoring

9.1 The council reserves the right to monitor and maintain logs of computer usage and inspect any files stored on its network, servers, computers, or associated technology to ensure compliance with this policy as well as relevant legislation. Internet, email, and computer usage is continually monitored as part of the council's protection against computer viruses, ongoing maintenance of the system, and when investigating faults.

9.2 The council will monitor the use of electronic communications and use of the internet in line with the Investigatory Powers Regulations 2018.

9.3 Monitoring of an employee's email and/or internet use will be conducted in accordance with an impact assessment that the council has carried out to ensure that monitoring is necessary and proportionate. Monitoring is in the council's legitimate interests and is to ensure that this policy is being complied with.

9.4 The information obtained through monitoring may be shared internally, including with relevant councillors and IT staff if access to the data is necessary for performance of their roles. The information may also be shared with external HR or legal advisers for the purposes of seeking professional advice. Any external advisers will have appropriate data protection policies and protocols in place.

9.5 The information gathered through monitoring will be retained only long enough for any breach of this policy to come to light and for any investigation to be conducted.

9.6 Councillors, staff, and other authorised users have a number of rights in relation to their data, including the right to make a subject access request and the right to have data rectified or erased in some circumstances. You can find further details of these rights and how to exercise them in the council's data protection policy.

9.7 Such monitoring and the retrieval of the content of any messages may be for the purposes of checking whether the use of the system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigation of wrongful acts, or to comply with any legal obligation.

9.8 The council reserves the right to inspect all files stored on its computer systems in order to assure compliance with this policy. The council also reserves the right to monitor the types of sites being accessed and the extent and frequency of use of the internet at any time, both inside and outside of working hours to ensure that the system is not being abused and to protect the council from potential damage or disrepute.

9.9 Any use that the council considers to be ‘improper’, either in terms of the content or the amount of time spent on this, may result in disciplinary proceedings.

9.10 All computers will be periodically checked and scanned for unauthorised programmes and viruses.

10. Misuse

Misuse of IT systems and equipment is not in line with the council’s standards of conduct and will be taken seriously. Any inappropriate or unauthorised use may lead to formal action, including disciplinary proceedings or, in serious cases, dismissal.

11. Related Policies

This policy should be read in conjunction with the following:

Information and Data Protection Policy

Management of Transferable Data Policy

UK GDPR and Freedom of Information Act 2000

Data Protection Act 2018

Computer Misuse Act 1990

Members of staff should also refer to the Employee Handbook

Equality and Diversity Policy

Accessibility regulations 2018

Equality Act 2010

WCAG 2.1 AA Minimum – moving to WCAG 2.2

Saltash Town Council Employee Handbook

Saltash Town Council Social Media Policy

Saltash Town Council Communications Policy and Strategy

Saltash Town Council Data Protection and Retention Policies

Appendix A

IT Equipment Collection Form

Name:	Position:
Device:	Model:
Asset Number:	Serial Number:
Condition**:** • New • Very Good • Good • Satisfactory	Accessories: • Wireless mouse • Laptop case • Charging lead
Details of any concerns with condition:	
Signatory:	
Date:	
Received By:	
Signature of Receiver:	
Date:	

I have read and agree to abide by the Provision of IT and Acceptable Use Policy.

I acknowledge that this device is the property of Saltash Town Council and should be returned immediately if I cease to be a Town Councillor.

I understand that any data on this device may be subject to release under the Freedom of Information Act 2000 and is subject to UK GDPR.

I acknowledge that I am responsible for repair or replacement costs if the damage or loss is due to negligence, misuse, or failure to follow proper handling and maintenance guidelines.

Saltash Town Council reserves the discretion to determine whether misuse, loss, or damage has occurred and retains the right to cover only a portion or none of the costs for repairing or replacing Saltash Town Council property in such cases.

In the event of loss or damage please report to the Office Manager / Assistant to the Town Clerk.

IT Equipment Return Form

Name:	Position:
Device:	Model:
Asset Number:	Serial Number:
Condition: • Excellent • Good • Fair • Poor • Damaged	Accessories: • Wireless mouse • Laptop case • Charging lead
If condition is poor / damaged please provide further information:	
Signatory:	
Date:	
Issued By:	
Signature of Issuer:	
Date:	

The Town Council reserves the discretion to determine whether misuse, loss, or damage has occurred and retains the right to cover only a portion or none of the costs for repairing or replacing Saltash Town Council property in such cases.

Appendix B

IT Equipment Incident Report Form

If Town Council equipment is lost, damaged or stolen please complete this form and return to the Office Manager / Assistant to the Town Clerk.

Information – To be completed by the Employee / Town Councillor

Name:
Department:
Position:

Incident Details

Date of Incident:
Time of Incident (if known):
Location of Incident:
Type of Equipment (Laptop, Phone, Tablet, etc.):
Asset Tag/Serial Number (if applicable):
Equipment Description (Brand, Model, Accessories, etc.):
Description of Incident: (Provide a brief explanation of how the incident occurred, including any relevant details such as witnesses, circumstances, or evidence.)

Action Taken

Was the incident reported to the police? [ ] Yes [ ] No If yes, provide the police report reference number:
Have IT been notified? [ ] Yes [ ] No
Any additional steps taken:

Employee / Town Councillor Acknowledgement

I confirm that the information provided is accurate to the best of my knowledge.

Signature:

Date:

For Office Use Only

Report Received By:

Date Received:

Action Taken:

Further Investigation Required: [ ] Yes [ ] No

Replacement/Recovery Plan: