Saltash Town Council

Policy/Procedure: **Computer Access & Usage Policy – Library 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	**Approved by**	
Date		**Date of approval**	
Responsible Officer		**Minute reference**	
Responsible Committee		**Review date**	Annual to check compliance with CC

Version History			
Date	**Version**	**Author/Editor**	**Comments**
February 2019	1	CC/ajt	Required by CC re IT systems provided

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

Acceptable use of computing and networking facilities provided by Cornwall Council

This policy applies to IT facilities (software and hardware, including public access computers, staff computers, telephones and self-service kiosks) provided and maintained at Saltash Library by Cornwall Council.

Summary

Cornwall Council seeks to provide accessible, assured and affordable digital, computing and network facilities for the purpose of supporting and improving the delivery of high quality public services to the residents it serves. Damage or compromise to these systems will cause disruption and incur costly, negative impact on the delivery of public services. It may further result in a breach of the personal information entrusted to us by citizens. This policy therefore sets out the principles for acceptable usage of the Council's computing and networking facilities to help to avoid any such consequence. It aims to ensure that authorised service users from all organisations understand their responsibilities for using the network and systems in a lawful manner that avoids bringing the Council or its family of companies into disrepute.

Context : Background

Cornwall Council "the Council" provides computing and networking facilities to support the delivery of Council services. It provides these facilities for its employees, members, contractors and other third parties who require access to the Councils systems or information.

The Council has a duty to ensure that information is correctly and professionally managed in the interests of:

- Confidentiality - will only be accessible to authorised persons.
- Integrity – will be accurate and complete.
- Availability – will be readily accessible to authorised persons.

The Council must also ensure that it complies with all relevant legislation and standards. These may include but are not limited to:

- The Computer Misuse Act 1990
- The Data Protection Act 2018
- The General Data Protection Regulation (GDPR)
- Payment Card Industry Data Security Standard (PCI DSS)
- ISO27001
- Public Services Network (PSN) Code of Connection
- Information Governance Statement of Compliance (to include IG Toolkit)

Objectives

This policy sets out the correct, appropriate and expected use of the Councils computing and networking facilities to help ensure its safe and reliable operation.

Scope

In addition to its direct employees, the Council provides use of its computing and networking facilities to its extended family of companies and organisations in the greater interest of Cornwall. In doing so it must manage risk to its core business and citizen's information. This policy therefore applies to everybody who uses the computing and networking facilities provided by Cornwall Council regardless if they are its direct employees or not.

The term 'service user' applies to any individual with access to the Councils network or computing resources. The term 'computer' or 'computing resource' within this policy extends to devices such as tablets and smartphones as well as laptops and desktop computers.

Policy details

Computer & Network Access Principles

All service users acknowledge that their use of Council computing, networks and systems or any use of the Public Services Network (PSN) may be monitored and data accessed for compliance, investigation, legal and threat analysis purposes. Communications sent or received via the network may be intercepted or monitored for lawful purposes.

Access to all Council systems must be gained through a secure and Information Service (IS) approved authentication method, unique to, and identifiable of the individual.

To improve efficiency and service user experience the expiry of network passwords will now only be enforced every six months unless it is suspected that a credential has been stolen or otherwise compromised. In which case the specific password(s) will be reset immediately.

Passwords with a minimum length of 10 characters and recognised complexity rules will be applied for all standard service users. Passwords with a minimum length of 14 characters and recognised complexity rules will be applied to IS and other staff with elevated technical network privileges. The use of a second factor or other authentication means such as biometric may be applied where it is deemed a password alone is inappropriate or insufficient.

The Council must demonstrate that it adheres to the best practice principle of 'least privilege'. In practice this means that all individuals are granted access only to the systems, programs and information necessary to do their job. All access must therefore be regularly reviewed to ensure it remains appropriate.

All computer equipment used within the Council's corporate network environment will be procured, approved, appropriately configured and managed by IS. Any exception to this must be formally sanctioned and authorised by IS.

It is strictly prohibited to physically connect any unmanaged device (that is, a device which is not owned, supplied, configured and managed by the Council) to the Council's corporate network.

Access for approved third party organisations is available through secure and approved connections, as configured by IS. Temporary workers, teleworkers and contractors will have access to the necessary systems through a unique sign-on procedure which will be removed at the end of their employment.

All network communications and telephony equipment is managed by IS or contractors specifically authorised by IS. It is forbidden to attempt to tamper with any such equipment either physically or logically. It is strictly forbidden to attempt to connect any networking communications equipment which has not been authorised by IS to the corporate network.

Service User Responsibilities

All service users of the Councils computing facilities and network must ensure that:

- Any breaches or suspected security incidents concerning Council network or computing facilities must be reported to the IS Service Desk immediately
- You never divulge your passwords, PINs or any other unique authentication credential to anyone under any circumstance.
- Do not write down your passwords, PINs or any other unique authentication credential. Recognising that it is difficult to remember many complex passwords IS can provide you with a password manager app for generating and storing passwords securely. This is the only means by which you should please record them.
- Change your password immediately if you believe its confidentiality may have been compromised.
- Always 'screen lock' your device desktop when leaving it unattended.
- Never knowingly use facilities in a manner which may introduce security or operational risk to the environment.
- Never attempt to perform any unauthorised changes to Council IT systems.
- All data held on the Council systems may also be subject to Freedom of Information or Subject Access Requests. For this reason, personal use of Cornwall Council's 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 and may be punishable by 12 months' imprisonment.
- If you believe you have mistakenly been granted access to IT systems, information or resources which are not appropriate or authorised to you, please immediately report this as a possible incident. Do not under any circumstance 'explore' or attempt further access yourself.
- Do not facilitate or attempt to facilitate access for anyone else who is not authorised to access specific information or information systems.
- Never copy, store or transfer data or software owned by the Council to any unmanaged device without explicit written consent from the Asset Owner.
- Your login ID identifies you as an individual and holds you directly accountable for all actions which take place under your credential. A logged in session must therefore not be shared with anyone else. Those managing a shared mailbox and/or calendar resources on behalf of another individual must do this via approved delegated resource means and not by the direct sharing of an individual's login credentials. Where a 'remote desktop' session is required by an approved engineer to fix an IT problem, the session must not be left unsupervised and must be fully and correctly closed once it is no longer required.

Manager's responsibility

Managers must ensure that:

- All access levels to systems and information are correct and appropriate to the users' job role.
- Their staff access to the Council's network must be properly authorised through the starter/leaver process and promptly removed when no longer needed due to change of role or termination of employment.
- Inform IS of any changes to a user's role or employment status which is relevant to the access which they have previously been granted.
- Council property is returned by the user upon termination of their employment, contract or agreement. This includes mobile phone, laptop, identity card/entrance card, any keys or other equipment belonging to the Council and in the possession of the leaver.
- Your staff are adequately IT trained to perform their role efficiently and securely.
- Take action when a member of staff within your service/team is believed to have breached policy.

Policy management

Authority is delegated to the Head of Governance and Information to undertake amendments of an administrative nature as are necessary, or to secure continuing compliance with the law.

Any changes to this policy will be communicated throughout the organisation using appropriate communication channels.

This policy will be circulated via the Council's policy dissemination tool and will be available on the Information Governance pages of the Intranet.

Breaches and non-compliance

Where external service providers, agents or contractors breach the policy, this should be addressed through contract arrangements.

Where the public have access to a Council system, if there is an actual or likely breach of information security, that access will be withdrawn until adequate controls are in place.

If you see or are aware of a breach of this policy, you must report it using the security incident reporting form.

Evaluation and review

This Policy will be reviewed by the Customer and Support Services SLT biannually.

Authority is delegated to the Customer and Support Services SLT to undertake amendments of an administrative nature as are necessary, or to secure continuing compliance with the law.