Saltash Town Council

Policy/Procedure: **Information Storage Policy - Library**

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**	

Version History			
Date	**Version**	**Author/Editor**	**Comments**
March 2019	1	CC/ajt	Required policy for Library

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

Information Storage Policy – Saltash Library

This policy applies to information stored on IT facilities provided and maintained at Saltash Library by Cornwall Council. This will normally be information related directly to the operation of the library service for which compliance with this policy is required by Cornwall Council. Relevant Cornwall Council policies are referenced in this document.

Summary

- The Council recognises the importance of storing information securely and in a manner which makes it accessible when it is needed.
- Users should store current physical (paper-based) information near their work area for easy access and make sure that their information storage area is not at risk from fire or flood.
- Users should operate a clear desk policy at all times and should use screen protectors when dealing with special categories of data
- When the cost or risk of storing semi-current physical information locally outweighs the benefits, users should arrange to move it to an approved storage area – the Council currently uses ReStore.
- Users must send permanent physical information to the Council's Records Office for archival storage.
- Records that no longer need to be kept for operational or statutory reasons should be reviewed by responsible staff before they are destroyed or sent to the Cornwall Record Office for preservation.
- Users must store current structured electronic information in databases such as MOSAiC for social care information and Academy for Revenues and Assessments information. Information Services (IS) can provide a list of approved database suppliers and provide appropriate storage devices.
- Users can store current unstructured electronic information in these areas:
    - Shared group areas - G: Drive
    - Private Home Drive - H: Drive

Context:

Background

The Council recognises the importance of storing information securely and in a manner which makes it accessible when it is needed. Access to information is essential for the Council's operational business and performance management. We also need to ensure that information which is end of life can be easily identified and disposed of.

Objectives

The objective of this policy is to provide a framework for decisions on the storing of information in the systems used by Cornwall Council. This is intended to allow effective decisions to be taken on the storage of all information and data which the council needs for its activities.

Distribution and Scope

This policy applies to anyone who processes information, for the Council or on behalf of the Council, and they must either adopt this policy or prove that they have equivalent policies in place.

Policy details:

Physical information – current

Current physical information is paper based information that is used frequently.

Users should store it near their work area for easy access and make sure that their information storage area will not be at risk from fire or flood.

Users must ensure that appropriate security measures are in place to protect the information (e.g. locking personal or sensitive information away when not in use).

Users must have an indexing system to make it easy for other users to find the information they need. Make sure that anyone who uses the information is trained in the system.

Users must regularly review the information they hold and dispose of it in line with relevant retention and disposal schedules, such as Batchelor, or the NHS or European Structural & Investment Funds or other specific guidance as appropriate.

Physical information – semi current

Semi current physical information is paper based information that isn't used frequently but still has to be kept to meet the retention guidelines.

When the cost or risk of storing this information locally outweighs the benefits, users should arrange to move it to an approved storage area. The Council currently uses ReStore to store semi-current physical information.

To access this service, follow the Archiving and Document Storage procedures on the Intranet.

Physical information – permanent

Permanent physical information is paper based information that is no longer needed for business purposes but still has to be kept. For example, there is an automatic requirement to preserve records of Council decisions.

Users must send this type of information to the Cornwall Records Office for permanent storage.

No longer needed

Records that no longer need to be kept for operational or statutory reasons should be reviewed by responsible staff before they are destroyed or sent to the Cornwall Records Office for preservation.

The most appropriate way to destroy records will depend on the information they contain. If they are confidential or contain personal or sensitive information, the records should be placed in the confidential waste bins provided at office locations or cross-cut shredded.

Relevant retention schedules will detail the records that should be sent to the Cornwall Records Office for preservation. These include documents that are of historical interest even if they are not needed for other purposes.

IF THE DATA IS NO LONGER NEEDED AND NOT PASSED TO CORNWALL RECORDS OFFICE IT SHOULD BE DESTROYED

Electronic information – current structured information

Current structured electronic information is electronic information that is used frequently.

Users must store corporate and departmental current structured electronic information in databases, for example, in MOSAiC for social care information and Academy for Revenues and Assessments information. Information Services (IS) can provide a list of approved database suppliers and provide appropriate storage devices.

IS takes backups to recover live databases, however, it is the Information Asset Owner's responsibility to ensure archived data is secure and accessible for as long as it has to be retained.

Electronic information – current unstructured information

Users can store current unstructured electronic information such as draft reports and meeting minutes and agendas in the following areas:

Shared group area (G: drive)

Users should use the shared drive (e.g. the G: drive) to store business information that they need to share with colleagues. This includes emails (see the Email Code of Practice), information generated from Microsoft products, information received from outside of the Council and draft material prior to publication.

There is limited storage space on the shared drive, so try to keep your file size down by making time to routinely weed information from electronic files. Where possible, do

not store any personal information on the shared drive, as others may be able to access it. Information should be secured via access controls to areas of the G: Drive and password protection if additional security is required.

A user's service will have its own folder structure on the shared drive, with appropriate security:

An Information Asset Owner nominated by each service will be in control of the design of the service's folder structure.

Other staff may be delegated to look after parts of the structure.

Every folder must have a Regulator, who will control security access, monitor content and dispose of information that is no longer needed, in line with appropriate retention guidelines.

Access to specific folders can be restricted to one person or a group of people. IS will set up appropriate controls at the request of nominated service staff.

The shared drive is backed up regularly to make it easier to recover current unstructured information.

Private home drive (H: drive)

Users' private drive (e.g. the H: drive) can only be accessed via their user login.

It should only be used for:

- Personnel information – Business information about individual employees, e.g. Performance Development System (PDS) information.
- EDRMS – RKYV – Information checked out for editing purposes from the EDRMS – (Electronic Document Records Management System).

Users should delete private information as soon as they are finished with it, making sure they don't keep it for longer than one month.

Private drives are backed up regularly to make it easy to recover current unstructured content.

Case management systems

Users must follow the processes and procedures associated with the relevant case management system e.g. Iken for Legal Services information. Case management systems should have appropriate retention and disposal rules applied.

Website and Intranet

Documents and files that are linked to the Council's Website and Intranet pages are stored and managed in the Media section of the content management editing tool.

Electronic Information - structured and unstructured – semi current and permanent

There is currently no corporate strategy or policy for these information types.

Policy Management

The Assurance Service in the Customer and Support Services Directorate is the designated Council owner of the Information Storage Policy and is responsible for the maintenance and review of the Policy, advice and guidelines.

The Council's Senior Information Risk Owner is responsible for managing corporate information risks, including maintaining and reviewing an information risk register.

The Council's Caldicott Guardian is responsible for protecting the confidentiality of service user information to ensure that standards are met when handling personal information in health and social care.

The Council's Information Governance Board meets on a regular basis to review all information governance and security related matters. Its membership includes the SIRO and Caldicott Guardian.

Service Directors and managers are responsible for ensuring that staff are made aware of and comply with the Information Storage Policy, Standards, Guidelines and Procedures.

The Council's Internal Audit Service will review the adequacy of the controls that are implemented to protect the Council's information and recommend improvements where deficiencies are found.

Users accessing Council information are required to adhere to the Information Storage Policy, Standards, Guidelines and Procedures.

Failure to comply with the Information Storage Policy, Standards, Guidelines and Procedures may lead to disciplinary or remedial action.

How the impact of this policy will be measured

The Corporate and Information Governance Team will monitor compliance with the policy and performance with regard to information storage.

Indicators to monitor the performance on information storage are:

- Audits to ensure effectiveness of procedures that provide a moderate level of assurance;
- Number of adverse judgements from the ICO linked to information storage issues.

Potential risks will be regularly monitored and evaluated to ensure this policy is kept up to date.

Wherever possible, this policy must be reviewed 3 months prior to new legislation taking effect. If that is not possible, because e.g. the new legislation is brought into effect without 3 months' notice, this policy must be reviewed within one month of the legislation being brought into effect.

Breaches and non-compliance

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

Breaching the Data Protection Act could lead to fines of up to £500,000 being issued by the Information Commissioner's Office, and possible criminal or civil action being taken against the Council or the individual(s) involved.

A breach of this policy must be reported using the information security incident reporting procedure.

Evaluation and review

This policy will be reviewed annually or as demanded by business need by the management team of the Assurance Service and the Information Governance Board.

This policy will be signed off by the Chair of the Information Governance Board.

Further information

Further information about this policy is available from the Corporate and Information Governance team in the Assurance service of the Customer and Support Services Directorate.

A mandatory online training module called Information Governance 2017 is available to ensure that all staff are aware of their obligations around information rights legislation (Data Protection, Freedom of Information, etc) and Information Lifecycle.

This policy should be read in conjunction with the following Council policies, procedures or guidance:

- Archiving and Document Storage Procedures
- Information Security Policy

- Information Security breach reporting procedure
- Information Storage Policy
- Subject Access Request procedure
- Data Quality Policy
- Freedom of Information Policy
- Information Lifecycle Policy
- Confidentiality Policy