Saltash Town Council

Policy/Procedure: **Information Security 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 from CC document

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

Information Security Policy - Library

This policy applies to the security of information at Saltash Library in relation to library services provided and maintained on behalf of Cornwall Council.

Summary

In order to operate legally and effectively, the Council must have confidence that its information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Necessary steps must therefore be taken to protect information systems and assets from unauthorised use, modification, disclosure or destruction, whether accidental or intentional. Furthermore, good information security enables us to better achieve the Council's strategic objectives whilst maintaining the trust of our partners and citizens.

Distribution - who needs to be aware of this policy

This policy applies to all staff and all Council information assets. Anyone who processes information for the Council or on our behalf, must either adopt this policy or demonstrate that they have equivalent policies in place.

Context

Background - why this policy is needed

Cornwall Council recognises that information is a valuable resource and seeks to lead and foster a culture that values, protects and uses information for public good. In order to carry out its statutory duties, the Council processes high volumes of information every day. This often includes confidential information about businesses and individuals. Service delivery and business continuity are further dependent on the integrity and continued availability of the Council's information systems.

In order to operate legally and effectively, the Council must have confidence that its information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users. Necessary steps must therefore be taken to protect information systems and assets from unauthorised use, modification, disclosure or destruction, whether accidental or intentional. Furthermore, good information security enables us to better achieve the Council's strategic objectives whilst maintaining the trust of our partners and citizens.

Objectives - what the policy aims to achieve

This policy is the overarching policy for the Council's Information Security Management System (ISMS). It sets out the highest level statements of intent by the Council and briefly describes the roles, structures and universal principles required to support these aims.

It is further supported by more detailed policies which prescribe more specific expectations around particular systems or business activities (such as email or mobile working for example).

Scope – what the policy covers

This policy applies to all staff and all Council information assets. Anyone who processes information, for the Council or on our behalf must either adopt this policy or demonstrate that they have equivalent policies in place.

Policy details

In order to protect the availability, integrity and confidentiality of the information under its control, Cornwall Council is committed and ultimately accountable at its most senior leadership levels to principles of Information Security and Assurance. The Council will therefore, at all times, have an appointed Senior Information Risk Owner (SIRO) at Corporate Director Level.

It is the duty of all staff to proactively uphold the Council's security principles and to understand their own responsibilities as described in the Council's Employee Code of Conduct and elaborated upon by the Council's current set of security policies.

All breaches of data security, accidental or otherwise, must be reported using the Information Security Reporting form on the Council's Intranet. Incidents will be investigated where appropriate. Suspected cyber-attacks (including viruses or malicious or otherwise unusual computer activity) must always be reported, in the first instance, to the IS Service Desk.

An" information asset" is a collective body of information, defined and managed as a single unit so it can be understood, shared, protected and used effectively. Examples include databases such as Mosaic (social care), Academy (revenues and benefits) as well as network 'drives' or portals containing collections of electronic files or structured paper held files.

The Senior Information Asset Owner (SIAO) is ultimately accountable for all of the assets collected, created, modified by or otherwise processed by their service or directorate. The SIAO must, therefore, be at least the Assistant Head of that service or Directorate (i.e. Tier 4 or above) and must be appropriately trained regarding their responsibilities as an SIAO.

The SIAO may delegate operational responsibilities to suitably competent practitioners to ensure that the information assets under their control are handled and managed appropriately. This will include making sure that information assets are properly protected and that their value to the Council and to the public are fully exploited.

Access to information systems must be determined by business requirements. Access shall be granted or arrangements made for users according to their role, only to a level that will allow them to effectively carry out their duties. SIAOs and those they delegate to are responsible for ensuring that the correct levels of access are granted.

The Council will comply with the legislative and regulatory requirements placed on it by outside bodies. These include but may not be limited to

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

It will further seek to align its practices with the ISO 27000 family of standards wherever possible.

Information Security education and training is to be made available to all Members and employees as appropriate, at the right level. It will also keep staff regularly informed of relevant security related information through corporate communications channels.

There are online training programmes available on Learning Pool.

Management

The Governance and Information Service within the Communities and Organisational Development Directorate is the designated Council owner of the Information Security Policy and is responsible for the maintenance and review of the Information Security Policy, Standards, Guidelines and Procedures.

The Council's Senior Information Risk Owner (SIRO) 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 the Caldicott Guardian.

Heads of Service, SIAOs and directorate managers are responsible for ensuring that staff are made aware of and comply with the Information Security 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 Security Policy, Standards, Guidelines and Procedures.

Breaches and non-compliance

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

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

How the impact of the policy will be measured

The Information Governance (IG) Board will monitor compliance with the policy and performance with regard to information security. Indicators to monitor the performance on information security are:

- Adherence to and progress towards recognised standards such as ISO 27001, IG Statement of Compliance (to include IG Toolkit) Public Services Network (PSN) Code of Connection, the Payment Card Industry Data Security Standard (PCI DSS).
- Metrics regarding the uptake and completion of training
- Formal audits and spot checks upon security controls and practice
- Metrics from controlled phish attack tests and reduced numbers of responses.

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

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