Sefton Council

Information Security Policy

Chapter 12

Asset Management

Author: Policy & Strategy Team
Version: 0.5
Date: April 2008

Document Control Information	
Document ID	
Document title	Sefton Council Asset Management Policy
Version	0.5
Status	Draft for comment
Author	R.Roscoe
Job title	Data Protection and Information Security Officer
Department	Information Services Policy and Strategy
Publication date	
Approved by	
Next review date	
Distribution	

Contents

1. Asset Management

1.1. Overview

For information systems to be used effectively, efficiently and legally the assets that make up those systems must be properly controlled. This is referred to as asset management.

Asset management is not limited to covering the stocks of information (electronic data or paper records) that the Council maintains. It also addresses the people that use them, the processes they follow and the physical computer equipment used to access them. Any asset management policy should address all these areas as they can all limit the confidentiality, quality and availability of information.

The following Policy details the basic requirements and responsibilities for the proper management of information assets at Sefton Council.

1.2. Policy Statement

The purpose of this policy is to achieve and maintain appropriate protection of organisational assets. It does this by ensuring that every information asset has an owner and that the nature and value of each asset is fully understood. It also ensures that the boundaries of acceptable use are clearly defined for anyone that has access to the information.

1.3. Scope of the Policy

This policy applies to all the systems, people and business processes that make up the Council's information systems.

2. Asset Management Requirements

2.1. Definition of important information assets

The process of identifying important information assets should be sensible and pragmatic. The Council has vast uncontrolled stocks of information. Items of information that have no security classification (See section 2.5) and are of limited practical value do not need a formal owner or inventory.

Important information assets will include:

- filing cabinets and stores containing paper records
- computer databases
- data files and folders
- software licenses
- physical assets (computer equipment and accessories, PDAs, cell phones)
- key services
- key people
- intangible assets such as reputation and brand

2.2. Inventory of Information Assets

The organisation must draw up and maintain inventories of all important information assets that it relies upon. These should identify each asset and all associated data required for risk assessment, information/records management and disaster recovery. At minimum it must include the type, location, designated owner, security classification (See section 2.5), format, backup and licensing information.

2.3. Assigning Asset Owners

All important information assets must have a nominated owner and should be accounted for. An owner must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner's responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

2.3.1. Unclassified and trivial information assets

Items of information that have no security classification (See section 2.5) and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department too ensure that this is done. Details of how to approach this task are available in the FOI resources page of the intranet.

2.3.2. Information assets with short term or localised use

For new documents that have a specific, short term, localised use, the creator of the document will be the originator. This includes letters, spreadsheets and reports created by staff. All staff must be informed of their responsibility for the documents they create. Specific requirements are highlighted in the Records Management Policy available on the intranet.

2.3.3. Corporate information assets

For information assets whose use throughout the Council is widespread and whose origination is as a result of a group or strategic decision, a corporate owner must be designated and the responsibility clearly documented. This should be the person who uses it the most, or has the most control over it.

2.4. Acceptable use of information assets

The Council must document, implement and circulate Acceptable Use Policies (AUP) for information assets, systems and services. These should apply to employees, contractors and third parties and use of the system must be conditional on acceptance of the appropriate AUP. This requirement must be formally agreed and auditable.

At minimum this will include e-mail and internet usage, mobile devices (telephones, PDAs and laptops) and usage of information beyond the Council's fixed perimeter (home working, VPN access, Portals).

2.5. Information classification (PERSONAL, CONFIDENTIAL, UNCLASSIFIED)

On creation, all information assets must be assessed and classified by the owner according to their content. At minimum all information assets must be classified and labelled if they are personal or confidential. The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification.

Classification alone is only a pointer. There are different degrees of personal and confidential and access and appropriate protection and use of information will be determined by risk assessment by the owner.

2.5.1. Personal Information

Personal information is any information about living, identifiable individual. The Council is legally responsible for it. Its storage, protection and use are governed by the Data Protection Act 1998. Details of specific requirements are in Chapter 3 - Data Protection Policy.

2.5.2. Confidential Information

Confidential information is any information for which the Council has a legal duty to protect. This is normally as a result of a contractual agreement, copyright and intellectual property issues. Definition of confidential should be as defined in the Freedom of Information Act 2000. For advice and assistance see below.

2.5.3. Unclassified information

Anything that is not either personal or confidential should be considered public. The Freedom of Information Act 2000 gives the public a right of access to all information held by a public body unless there is a valid exemption in the Act that allows them to withhold it. The two main exemptions used are confidentiality and personal information*. An 'internal' classification is therefore meaningless.

* There are other exemptions. For advice and assistance on classification see the FOI resources page on the intranet or contact the Information Owner, the Data Protection Officer (4416) or the Caldicott Guardian (3774).

2.6. Sharing classified information with other organisations

There is at present no simple common data classification scheme that is practically applied across the public sector. To avoid confusion where classified Council information is to be shared with or transferred to different organisations it is essential that both parties must understand any classification system in place at the other end. Non-disclosure agreements must be in place where appropriate (See 2.7 below).

Any sharing or transfer of Council information with other organisations must comply with all Legal, Regulatory and Council Policy requirements. In particular this must be compliant with the Data Protection Act 2000, The Human Rights Act 2000 and the Common Law of Confidentiality.

A detailed summary of how to transfer Council Information securely can be found in the Secure Transfer of Information Policy available on the intranet. For advice and assistance on whether to share Council Information see the FOI resources page on the intranet or contact the Information Owner, Data Protection Officer (4416) or the Caldicott Guardian (3774).

2.7. Non-disclosure Agreements and Information Sharing Protocols

Where the Council needs to share classified information with a third party organisation an appropriate risk assessment must be carried out and the results of this must be reflected in a non-disclosure agreement that the third party is required to sign. This must be drafted by a legal specialist and should contain details of controls required to ensure that the organisation is able to respect the classification of the information being shared.

Where regular sharing of classified information between the Council and other organisations is required then an Information Sharing Protocol must be agreed between the organisations. For advice and assistance on Information Sharing protocols, contact the Information Owner, Data Protection Officer (4416) or the Caldicott Guardian (3774).

2.8. Information labelling, handling and disposal

The Council must implement a set of procedures for appropriate information labelling and handling that reflects the information classification scheme above. It must cover all formats of information, both physical and electronic. The labelling must inform the user of the contents without revealing unnecessary details or attracting attention. These procedures must cover the processes for acquisition, copying, chain of custody, logging security events, storage, transmission, transfer and ultimate destruction of information.

Detailed requirements for secure handling and disposal of classified information are contained in the Records Management Policy available on the intranet. Detailed requirements for the transfer of confidential and personal information are contained in the Secure Transfer of Information Policy and the Records Management Policy.

2.9. Legal disclaimers

Faxes and e-mails are widely used to transfer information. Both can be unreliable and subject to user error so there is a high risk of deliberate or accidental delivery to the wrong address. Policies must be established on the use of such mechanisms, and all such messages should carry a standard disclaimer clearly printed on the fax cover sheet and it should be a procedural requirement that all faxes include a standard cover sheet. The disclaimer must cover:

- A statement that the information is classified and for the addressee only.
- Request that the recipient to notify the sender immediately if they are not the correct recipient.
- A statement to cover liability for errors or omissions in transmission.
- A statement that any opinions are those of the author and do not reflect in any way those of the organisation.

Any disclaimer used must be approved by the Legal department to ensure compliance with current legislation.

2.10. Policy Compliance

If you are found to have breached this policy, you may be subject to the Council's disciplinary procedure. If you have broken the law, you may be subject to prosecution.

If you do not understand the implications of this policy or how it may apply to you, seek advice from the Information Services Department via the IS Helpdesk on 0151 934 4999.