

Cobseo – The Confederation of Service Charities

Data Classification, Handling and Disposal Policy

Purpose

The purpose of this policy is to define a system of categorising information in relation to its sensitivity and confidentiality, and to define associated rules for the handling of each category of information to ensure the appropriate level of security (confidentiality, integrity and availability) of that information.

The policy aims to:

Protect information from accidental or deliberate compromise, which may lead to damage, and/or be a criminal offence.

Help to meet legal, ethical and statutory obligations.

Protect the interests of all those who have dealings with the Confederation and about whom it may hold information (including its Members, employees and service provider and/or business contacts etc.)

Promote good practice in relation to information handling.

Scope

This policy covers all information held by the Confederation and the handling rules mentioned shall apply to all employees of the Confederation and to third parties handling Member information.

Relationship with Existing Policies

This policy forms part of the Confederation's Information Security Policy. It should be read in conjunction with the Information Security Policy and all other supporting data protection policies.

Policy Statement

All employees of Confederation and third parties who handle Member information on behalf of the Confederation have a personal responsibility for ensuring that appropriate security controls are applied in respect of the information they are handling for the Confederation. Appropriate security controls may vary according to the classification of the information and the handling rules for the relevant category shall be followed.

Automatic technical controls may be implemented to assist users in complying with these controls, but where technical measures are not implemented users are responsible for complying with this policy. Please see Annex 1.

Cobseo – The Confederation of Service Charities

Data Classification, Handling and Disposal Policy

Policy

Information shall be handled in accordance with the Information Handling Rules (Annex 1) and where information falls within more than one category, the higher level of protection shall apply in each case.

Where a third party will be responsible for handling information on behalf of the Confederation, the third party shall be required to adhere to this policy prior to the sharing of that information.

Where the Confederation holds information on behalf of another organisation with its own information classification, written agreement shall be reached as to which set of handling rules shall apply prior to the sharing of that information

Responsibilities

The Director of Operations shall ensure that the Information Classification and associated Handling Rules are reviewed regularly to ensure they remain fit for purpose.

It shall be the responsibility of every individual handling information covered by this policy, to mark classified material as such, to apply the appropriate handling rules to each category of information, and to seek clarification or advice from the Director of Operations where they are unsure as to how to label or handle information.

All employees of the Confederation shall report issues of concern in relation to the application of this policy, including alleged non-compliance, to the Director of Operations.

Compliance

Breaches of this policy may be treated as a disciplinary matter dealt with under the Confederation's staff disciplinary policies or the Confederation's Executive Committee. Where third parties are involved breach of this policy may also constitute breach of contract.

Cobseo – The Confederation of Service Charities

Data Classification, Handling and Disposal Policy

Annex 1 – Information Handling Rules

Class	Description	Storage	Dissemination and Access	Exchange and Collaboration	Disposal
Public	Information that can be seen by anyone.	Electronic information should be stored using the Confederation's IT facilities to ensure appropriate management, backup and access.	Information can be shared via the web without requiring Member access. Electronic and hard copy information can be circulated freely subject to applicable laws e.g. copyright, contract, competition.	Information can be exchanged via email or file sharing without needing encryption.	Electronic equipment and printed copies holding this information must be disposed of in accordance with any retention schedule.
Restricted	Non-confidential information where dissemination is restricted in some way e.g. restricted to Members of the Confederation.		Information can be shared via the web, but the user must provide Membership authentication or a federated authentication. May be accessed remotely and via disk-encrypted portable and mobile devices without further encryption.		
Confidential	Sensitive information e.g. personal data, commercial or legal information, or information under embargo prior to wider release. Includes data about individuals, and data about an institution.	Information must be stored using the Confederation's IT facilities. Portable devices must have full disk encryption. Storage on Personally owned (e.g. home) computer is NOT permitted.	Access to confidential data must be strictly controlled by the Data Owner who should conduct regular access reviews. For web access, encryption must be used. Confidential data must not be extracted from the Confederation's IT systems and stored on local IT systems. If a portable device (e.g. a laptop, tablet or phone) is used to access confidential information, the device must be encrypted and require a password or PIN to access. Access to confidential data from outside the Confederation's office must comply with the above conditions.	The method to be used for exchanging confidential information must take account of the nature and volume of the data to be exchanged so that the impact of inappropriate disclosure can be assessed, and an appropriate method selected.	