Asset Management Policy

Version number:	2.0
Consultation Groups	Information Governance Steering Group, Digital Board and Key Leads
Approved by (Sponsor Group)	Information Governance Steering Group, Digital Board and Key Leads
Ratified by:	Quality Committee
Date ratified:	30th August 2022
Name of originator/author:	Michael Loughlin
Executive Director lead:	Phillipa Graves
Implementation Date:	September 2022
Last Review Date	February 2024
Next Review date:	February 2025

Services	**Applicable**
Trust wide	X
Mental Health and LD	
Community Health Services	

Version Control Summary

Version	Date	Author	Status	Comment
1.0	30/08/2022	Michael Loughlin	Draft	Initial Draft
2.0	07/02/2024	Octavius Max-Lino	Final	Review

Contents

1 Introduction

ELFT has a wide variety of assets under its control, all of which have specific value and requirements for protection. In order to provide effective information security, it is important that assets are identified and responsibility for their protection is allocated correctly.

These responsibilities include ensuring assets are handled and used appropriately, returned or disposed of when no longer required, and that appropriate controls are placed upon them in line with their sensitivity and value to the organisation.

This policy sets out the main rules for the management of assets and will be supported by more specific procedures which detail how these rules must be implemented.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to ELFT systems.

The following policies and procedures are relevant to this document:

- *Information Classification Procedure.*
- *Information Labelling Procedure.*
- *Procedure for the Management of Removable Media.*
- *Asset Handling Procedure.*
- *Backup Policy.*
- *Teleworking Policy.*

2 Asset management policy

2.1 Responsibility for assets

An inventory of assets associated with information and information processing facilities within ELFT will be maintained. The types of assets to be identified and controlled will include:

- Information
- Cloud service customer data
- Cloud service derived data
- Hardware
- Software
- Physical
- Services
- People
- Other

These assets may be recorded in more than one location or system, for example hardware and software may be automatically tracked using configuration management tools. The asset inventory will provide input to the risk management process to ensure that risks to all ELFT business-critical assets are considered.

Each asset recorded in the inventory will be assigned an agreed owner who will ensure that:

- All assets under their ownership are included in the inventory
- An appropriate classification is assigned to the assets
- Access to the assets is controlled appropriately and reviewed periodically.
- Assets are handled correctly, including their disposal

The asset owner may be an individual, a role or an organisational unit. Day to day operation and maintenance of the asset may be delegated by the owner to a custodian. Rules for the secure use of the assets will be defined by the owner and communicated to those who have access to them.

Upon termination of employment or third-party contracts, all assets that have been issued to the terminated party must be returned to ELFT including the secure removal of organisation data from personal equipment.

2.2 Information classification

All information within ELFT will be subject to security classification. The information classification scheme requires information assets to be protectively marked as one of three classifications (excluding public information which does not need to be marked). The way the information is handled, published, moved and stored will be dependent on this scheme.

The classes of information are:

- Level 1: Protected
- Level 2: Restricted
- Level 3: Confidential

The decision regarding which classification an information asset should fall into will be based on the following main criteria:

1. Legal requirements that must be complied with
2. Value to the organisation
3. Criticality to the organisation
4. Sensitivity to unauthorised disclosure or modification

All classified information must be clearly labelled with the classification that has been assigned, so that employees, contractors and third parties are aware of the level of protection that must be applied, in accordance with ELFT procedures.

2.3 Media handling

Removable media (for example CD, DVD, memory stick) must not be used to store classified information unless its use is authorised by the CISO.

Where there is a requirement for data transfer to third parties, a secure method will be arranged by the Digital Service Desk. Where this is not possible encrypted PIN Keypad removable media may be used with the approval of the CISO. For highly classified information, this must be physically taken to the third party by an organisation employee. For lower classifications, it may be sent by registered courier with a tracking facility and requiring a signature at the other end.

Employees and contractors must not save organisation data to memory stick, CD or other removable media as backups, to take data to a third-party site, or in order to take it home to work on using their own computer, without the prior approval of the CISO.