NHS
East London
NHS Foundation Trust

Acceptable Use 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:	30/08/2022
Name of originator/author:	Michael Loughlin
Executive Director lead:	Phillipa Graves
Implementation Date:	September 2022
Last Review Date	September 2024
Next Review date:	September 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	September 2024	Octavius Max-Lino	Final	Reviewed.

Contents

1 Introduction 1

2 Acceptable use Policy 2

1 Introduction

ELFT takes the subject of information security very seriously. We have a duty to protect the information that we collect and use for the benefit of the organization and its customers. As an employee, you will be expected to comply fully with all of the information security policies that are in place and to report any breaches of these policies of which you may become aware.

This document gives a summary of the main points of the relevant policies and asks you to sign to say that you have read it and understand its provisions.

Anyone breaching information security policy may be subject to disciplinary action. If a criminal offence has been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, please seek advice from your immediate manager in the first instance.

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 Security Policy*
- *Electronic Messaging Policy*
- *Internet Acceptable Use Policy*
- *Mobile Device Policy*
- *Teleworking Policy*
- *Privacy and Personal Data Protection Policy*
- *Cloud Computing Policy*
- *Asset Handling Procedure*
- *Software Policy*
- *Access Control Policy*
- *Anti-Malware Policy*
- *Information Security Incident Response Procedure*
- *IP and Copyright Compliance Policy*
- *Social Media Policy*
- *HR Security Policy*
- *Asset Management Policy*

2 Acceptable use policy

Please ensure you have read the following summary of the main points of the organisation's policies regarding information security.

1. I acknowledge that my use of ELFT computer and communications systems may be monitored and/or recorded for lawful purposes.
2. I accept that I am responsible for the use and protection of the user credentials with which I am provided (user account and password, access token or other items I may be provided with)
3. I will not use anyone else's user account and password to access company systems
4. I will not attempt to access any computer system to which I not been given access
5. I will protect any classified material sent, received, stored or processed by me according to the level of classification assigned to it, including both electronic and paper copies
6. I will ensure that I label any classified material that I create appropriately according to published guidelines so that it remains appropriately protected
7. I will not send classified information over the Internet via email or other methods unless appropriate methods (e.g., encryption) have been used to protect it from unauthorised access
8. I will always ensure that I enter the correct recipient email address(es) so that classified information is not compromised
9. I will ensure I am not overlooked by unauthorised people when working and will take appropriate care when printing classified information
10. I will securely store classified printed material and ensure it is correctly destroyed when no longer needed
11. I will not leave my computer unattended such that unauthorised access can be gained to information via my account while I am away
12. I will make myself familiar with the organisation's security policies and procedures and any special instructions relating to my work
13. I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security or if I observe any suspected information security weaknesses in systems or services
14. I will not attempt to bypass or subvert system security controls or to use them for any purpose other than that intended
15. I will not remove equipment or information from the organisation's premises without appropriate approval
16. I will take precautions to protect all computer media and mobile devices when carrying them outside my organization's premises (e.g., leaving a laptop unattended or on display in a car such that it would encourage an opportunist theft)
17. I will not introduce viruses or other malware into the system or network
18. I will not attempt to disable anti-virus protection provided at my computer
19. I will comply with the legal, statutory or contractual obligations that the organization informs me are relevant to my role
20. On leaving the organization, I will inform my manager prior to departure of any important information held in my account

Declaration

I have read the information security policy summary above and agree to comply with its contents and those of any other relevant policies of which the organization may make me aware.

Name of User:

Signature of User:

Date:

A copy of this statement should be retained by the User and ELFT.