

Business Unit	Corporate Services - ICT
Document Title	ICT Security Framework Policy
Document No.	ICT031/ICTSF/V3/24
Approved By	Chief Executive LWETB
Noted By	LWETB Board
Date Noted	October 2024

Longford and Westmeath Education and Training Board

ICT Security Framework Policy

Table of Contents		Page
1	Introduction	2
	1.1 Definitions used throughout the listed policies.....	2
	1.2 Scope.....	4
	1.3 Privacy Concerns.....	4
2	Policies	5
	2.1 ICT Policies Overview.....	5
3	User Roles and Responsibilities	5
4	Relevant Statutes	5
5	Review and Implementation	7
6	Responsibilities	7
7	Ownership and Authorisation	7

1. Introduction

Longford and Westmeath Education & Training Board (LWETB) endeavours, at all times, to ensure consistent, high-quality implementations and management of its ICT resources, processes and practices. A comprehensive framework of well-defined policies, procedures and standards are required in order to achieve this. The need for formal ICT policies has been highlighted in risk management processes and internal control frameworks for LWETB. This ICT Security Framework Policy is a key element in meeting and supporting these requirements.

The objective of this policy is to ensure an organisation-wide approach to the establishment, implementation, operation, review, maintenance, and improvement of all aspects of Information security with reference to internationally recognised best practice. Its purpose is to communicate standards of care to ensure the consistent and appropriate protection of information throughout LWETB, and to meet the key business, legislative, regulative and group security requirements. The ICT policies may be read as a complete set or may be used as a reference point, depending upon need.

The owner of the ICT Framework is the Corporate Service, OSD. Concerns with the policy should be raised to the LWETB Corporate Service.

1.1 Definitions used throughout the listed policies

- **Asset Owner** – The person with overall responsibility for an asset, either hardware or software
- **Asset Tag** – An asset tag is a tag or label affixed to assets to identify each one individually and track data such as location or maintenance history
- **BCP** – “Business continuity planning” – the practice of planning and preparing to mitigate disruption due to service interruption
- **BYOD – “Bring Your Own Device”** - the practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for the purpose of performing employment duties
- **Corporate Data** – means all **data** maintained by LWETB including, but not limited to, data related to its finances, taxes, employees, customers, students, suppliers and the business
- **Data** - The term data refers to information including information stored or transmitted in electronic format
- **Device Management Solution** - is a type of management or security technology that enables IT administrators to monitor, manage and secure corporate or personally owned devices that run across multiple operating systems
- **Encryption** – the process of converting information so that it cannot be read by unauthorised people

- **Firewall** - Is a network security device, or computer-based software solution, that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of security rules
- **HTTPS** - Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer
- **Information** - The term information refers to knowledge which may be stored in any form, whether printed or in electronic form
- **Information Asset** – Information or Data that has value or is critical to the operation of LWETB
- **Malware / Virus** - A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software
- **MFA** – Multi-Factor Authentication, is a process whereby a user’s identity is further verified via phone call, authenticator application, secure fob or code sent by email, SMS or any secondary means of verifying a user’s identity
- **Must** – refers to an action that is an absolute requirement of the policies
- **Patch** – is a **software or operating system (OS) update that addresses security vulnerabilities within a program or product**
- **Phishing** - Is the practice of sending fraudulent communications that appear to come from a reputable source. It is usually performed through email
- **Processing** – means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- **Should** – refers to an action that ought to be applied. In certain circumstances, there may exist a valid reason to ignore a particular item. [In this case, the full implications must be understood, carefully weighed before choosing a different course];
- **Sensitive Data** – All data classified as commercially sensitive or privileged, or Special Category data as defined by the GDPR such that it is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation shall be prohibited
- **Personal Data** – as defined by the GDPR, means any information relating to an identified or identifiable natural person (‘data subject’);
 an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name,

 an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- **SIEM** – “**Security information and event management**” - real-time monitoring and analysis of events as well as tracking and logging of security data for compliance or auditing purposes

- **SOC – “Security operations centre”** is a centralised function within an organization or third party, employing people, processes, and technology to continuously monitor and improve an organisation's security posture while preventing, detecting, analysing, and responding to cybersecurity incidents
- **Syslog** - stands for System Logging Protocol and is a standard protocol used to send system log or event messages to a specific server, called a syslog server. It is primarily used to collect various device logs from several different machines in a central location for monitoring and review
- **Technology Infrastructure** – All computing, connectivity and cloud-hosted technology owned or managed by LWETB and its contracted third parties
- **TLS** – Transport Layer Security (TLS), is a security protocol that provides privacy and data integrity for internet communications
- **User** – refers to an employee, whether full or part time, contractor, intern, partner, consultant, external individual or organisation, and also captures a learner or student. Further:
 - Internal User – refers to a directly employed full-time or part-time staff member, intern, learner, student, parent/guardian of a learner or students under eighteen years of age
 - External User – comprehends contractors, partners and / or consultants, external individuals and organisations

1.2 Scope

This policy framework applies to all users as captured in the widest definition of user in the definitions section above. Users are responsible for reading the policies which are relevant to their respective work areas and familiarising themselves with contents thereof.

1.3 Privacy Concerns

LWETB operate to the standards set out by the data protection commissions General Data Protection Regulation (GDPR), Please contact the Data protection dept should you have any concerns regarding the management of your data within LWETB.

2. Policies

2.1 ICT Security Framework Policies Overview

A number of ICT policies have been developed to facilitate and ensure consistent, high-quality implementations and management of LWETB ICT resources and information. These policies and all other policies and procedures that are relevant are available on www.lwetb.ie or on request from the Corporate Service Department.

Always refer to the online document for the most up-to-date version of this document or other policies above, as available at: www.lwetb.ie.

3. Roles and Responsibilities

Information security is the responsibility of all LWETB users with access to ICT systems and data. LWETB is obliged to take breaches of policy seriously and it is incumbent upon us all to read and understand the security policies that apply when performing our duties. Any breaches of policies listed may result in disciplinary action for internal users, and, in the case of external users engaged by LWETB, may result in legal redress.

4. Relevant Statutes

LWETB is obliged to comply with relevant legal and regulatory requirements in respect of financial records, customer, and organisational personal data *etc.*

Relevant legislation in Ireland includes but is not limited to:

- Data Protection Acts 1988 to 2018
 LWETB has several legislative requirements in relation to the processing of personal data. This includes the collection, use of, retention of, security of personal data from unauthorised access, disclosure, destruction or accidental loss, and the requirement to fulfil Data Subject Right Requests. Privacy legislation also puts restrictions on privacy assigned to individuals and the level of user- data that can be monitored within LWETB
- Safety, Health, and Welfare at Work Act 2005
- Copyright and Related Rights Act 2000 (as amended)
- Criminal Damage Act 1991 and Criminal Justice (Theft and Fraud Offences) Act 2001
 Damage or threatened damage to data or ICT infrastructure is an offence. Any attempt to access or damage data or equipment to which a user has not been formally granted access may be a breach of this Act, and hence a prosecutable offence
- Child Trafficking and Pornography Act 1998 to 2004
 If a user views or receives any image(s) or media (picture, graphic, booklet, audio tape, video *etc.*) which depicts a child engaged in, or witnessing, a sexually explicit act, it must be reported to the Gardaí –
 this act has a mandatory reporting requirement for which there are no exceptions. Any such incident will be dealt with in accordance with the Child Protection Policy
- The Irish Constitution (Implicit right to personal privacy under Article 40.3.1)
- European Convention on Human Rights (Article 8)
- The Lisbon Treaty (Article 16)
- The European Charter on Human Rights (Article 8)
- ePrivacy Regulations 2011 (S.I. 336 of 2011)

The following are the relevant industry standards which were referenced in the drafting of ICT policies:

- PCI DSS
 Where payment card (credit/debit card) data is transmitted, stored or processed; the control and protection of that data must comply with PCI DSS (<https://www.pcisecuritystandards.org/>) standards.
- International Standards

The following international standards provide excellent baselines for implementation of an ICT framework policy, and security controls required. While it is not our intention to become ISO-27001 certified, this ICT framework is referenced to the following international standards for best practice information security governance, risk and compliance:

- ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems – Requirements
- ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security management
- ISO/IEC 27005:2008, Information technology — Security techniques – Information security risk management
- ISO/IEC 27031:2011, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 24762:2008, Security techniques — Guidelines for information and communications technology disaster recovery services
- ISO/IEC 31000:2009 Risk Management — Principles and Guidelines
- ISO/IEC 31010:2009 Risk management — Risk assessment techniques

5 Review and Implementation

This policy will be reviewed annually by the Senior Leadership Team in line with best practice, or in light of changes in legislation and guidance from sources such as Internal Audit, C&AG, The Department of Education, the Department of Further and Higher Education, Research, Innovation and Science and the Department of Public Expenditure & Reform. The date of implementation is the date of LWETB Chief Executive approval.

6 Responsibilities

Owner	Responsibilities
Director of Organisational Support & Development	Revisions and updates to the policy
LWETB Management Team	Approval of the Policy
Data Owners	Ensuring implementation of policy.
Internal and external audit	Monitoring and reporting compliance with the policy

7 Ownership and Authorisation

OWNER	DATE	SIGNATURE
<i>Organisation Support & Development Director</i>	Sep 23, 2024	<i>Charlie Mitchell</i> Charlie Mitchell (Sep 23, 2024 14:03 GMT+1)
AUTHORISED BY	DATE	SIGNATURE
<i>Chief Executive</i>	Sep 23, 2024	<i>Liz Lavery</i> Liz Lavery (Sep 23, 2024 14:52 GMT+1)