lwetb
Bord Oideachais agus Oiliúna an Longfoirt agus na hIarmhí
Longford and Westmeath Education and Training Board

Title	**LWETB Encryption Usage Policy**
Date	26th May, 2020
Approved	Chief Executive LWETB
Noted By	LWETB Board (26th May, 2020)

LWETB Encryption Usage Policy

1. Purpose

There are two types of information processed by LWETB, notably:

- Public Information intended for general public use and which would cause no harm to any individual, group, or to the organisation if made public

- Classified Information which refers to all other types of information processed within LWETB. This includes all forms of data which if lost, would be expected to have an adverse effect on LWETB operations, assets or individuals.

The purpose of the Encryption Policy is to establish principles to effectively and efficiently plan, prepare and deploy appropriate encryption solutions to secure LWETB classified information in line with LWETB policies (see list at the end of this policy), and specifically where encryption is mandated.

Please note if there is anything in this Policy which is unclear or if you have any questions please contact ICT Support who will provide assistance.

2. Description

LWETB defines Classified Information within LWETB as one of Controlled, Restricted and Highly Restricted classifications. The Data Handling policy defines the handling rules for each classification type, and details when encryption should be used.
This policy applies to:

- All Staff who have access to LWETB IT Systems
- All contractors, vendors or others (including 3rd parties), who have access to LWETB IT Systems.

It is the personal responsibility of each individual to read this and related security policies and be familiar with its contents. It is the responsibility of all Senior Management to ensure that all staff using LWETB IT systems are aware of and understand their responsibilities in respect of this policy.

3. Definitions

Classified Information refers to all information classified as one of:

- Controlled
- Restricted
- Highly Restricted

“Must”, or the terms **"required"** or **"shall"**, refer to an absolute requirement of the policy.
“Must not”, or the phrase **"shall not"**, refer to statements which are an absolute prohibition of the policy.

“Should”, or the adjective **"recommended"** refers to a statement that should 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 and carefully weighed before choosing a different course.
“**Should not**”, or the phrase "**not recommended**" mean the specified behaviour should not be performed. There may exist valid reasons in particular circumstances when the particular behaviour is acceptable, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

4. Requirements

If LWETB classified information is transferred or stored internally or externally to LWETB it must be encrypted in line with data handling rules. These include:

i. Wherever LWETB classified information (as defined above) is transferred or stored internally or externally to LWETB, it must be encrypted.
ii. Third parties, departments and business functions are all required to employ LWETB-approved encryption solutions prior to dealing with classified information, and at all times thereafter. This applies to both LWETB owned and privately owned devices (BYOD).
iii. Valid Encryption Methods are as follows:

(a) Full Disk Encryption
Full disk encryption encrypts all data on a system, including files, folders and the operating system. This is most appropriate when the physical security of the system is not assured. Examples include traveling laptops that are not in a physically secured area.

(b) E-mail Encryption
E-mail-specific products integrate encryption into the e-mail client, allowing messages and attachments to be sent in an encrypted form transparent to the user. This is most appropriate for departments whose users require frequent and regular encryption of e-mail communications.
Most departments can make use of a broader range of file/folder encryption products to encrypt individual files and folders.

(c) External Devices Encryption
External devices such as hard drives, DVDs, CDs and USB flash drives can be encrypted in their entirety. Data on these systems can be considered secure as long as access to the key and encryption software is restricted.

(d) File/Folder Encryption
Individual or multiple files or folders can be encrypted separate from the host operating system. These encrypted archives can be stored in different locations such as network shares, external hard drives or be transmitted securely via e-mail. This is prone to error, and where classified information is stored on the device, the preference is to use Full Disk Encryption.

(e) Mobile Device Encryption
Mobile devices such as tablets and smartphones allow users to exchange, transfer and store information from outside of the organisation. The extreme portability of these devices renders them susceptible to theft or loss. LWETB ICT therefore insists on the use of standardised devices such as laptops/tablets for storing, transmitting or processing LWETB classified information.

(f) Transport-Level Encryption
Secure transport client/server products provide transport-level encryption to protect data in transit between the sender and recipient in order to ensure delivery without eavesdropping, interception or forgery. This scenario requires the appropriate configuration of a server in order to allow clients to connect in a secure manner.

For applicable and preferred products for each encryption method please refer to LWETB ICT Support

iv. Passwords or encryption keys required to open encrypted files must be supplied to authorised personnel on request (if stored on the file system in encrypted format). All encryption key passwords must be stored securely in case they are required to reproduce the document.
v. All passwords stored electronically must be encrypted. Passwords must not be saved in clear text on a file or database for any purpose.
vi. Where password-based encryption is used, the password must never be transmitted in the same way as the encrypted file. For example, if an encrypted file is e-mailed, the password should be sent by another means such as SMS message.

5. Responsibilities

Owner	**Responsibilities**
Director of Organisation Support and Development	Revisions and updates to the Policy
LWETB Senior Leadership Team	Review of the Policy
LWETB Chief Executive	Approval of the Policy
All End-users	Responsible for implementation of the Policy
Internal and external audit	Monitoring and reporting compliance with the Policy
LWETB ICT Support	Tracking of calls related to security incidents

6. Related Documents

- Bring Your Own Device Policy
- Password Acceptable Usage Policy
- Data Handling and Classification Policy
  Logical Access Policy