Business Owner	**Organisation Support & Development**
Document Title:	**Bring Your Own Device Policy LWETB**
Document No.	**ICT002/BYOB/V3/2024**
Version:	**ETBI 1.5**
Approved By:	**Chief Executive LWETB**
Noted by:	**LWETB Board**
Date Noted:	**November 2024**

Longford and Westmeath Education & Training Board

Bring Your Own Device (BYOD) Policy

Contents

1 Introduction

1.1 Purpose of this Document

The BYOD policy is defined in the Longford and Westmeath Education and Training Board (LWETB) ICT Security Framework Policy and should be read in conjunction with all other ICT and Data Protection policies to ensure that required security standards are adhered to. This policy is intended to protect the security and integrity of the LWETB Corporate Data and technology infrastructure. It outlines and sets the standards and also the user's responsibilities to keep corporate data safe where LWETB consents to employees using personal devices for work purposes or where an employee consents to LWETB requests of the employee to use a personal device for work purposes.

1.2 Scope and Constraints

This policy applies to all users referred to in the definitions section accessing, storing, transmitting, or otherwise processing LWETB corporate data to or from a device not registered in LWETB Device management solution / personal device. This policy is effective as of the issue date and does not expire unless superseded by another policy. LWETB generally does not recommend use of personal devices for the access or retention of LWETB data. Where this is required, permission should be sought and approved by CS and/or ICT support services

By connecting to LWETB infrastructure, you are agreeing to the terms contained within this policy document.

BYOD devices include, but are not limited to the following:

- Laptops
- Desktops
- Smart-phones
- Tablets
- USB memory sticks
- Digital cameras
- Any device capable of connecting to LWETB infrastructure.

1.3 Definitions

A full range of definitions is available in the ICT Security Frameworks Policy.

2. BYOD Policy Overview

This policy outlines the standards required and upheld by LWETB as well as the responsibilities of users who wish to access LWETB Corporate Data from their own personal devices, or any device not registered within the LWETB device management platform. LWETB Users must agree to the terms and conditions set forth in this policy before connecting, or continuing to connect, their devices to the LWETB technology infrastructure.

LWETB will respect the privacy of personal devices and may only request access to the device by Corporate Services to implement security controls or to respond to FOI/GDPR requests or to comply with a discovery Court Order. It is the personal responsibility of each individual to read this and related ICT and Data Protection policies and be familiar with the contents therein. It is the responsibility of all managers to ensure all users of ICT systems are aware of and understand their responsibilities in this policy.

3. Requirements for BYOD devices

3.1 ICT Technical Standards

- All access to corporate data is made available using encrypted communications standards only see encryption policy for details.
- All access to Corporate Data requires the use of Multi-Factor Authentication (MFA) (see Remote Access for Staff Policy for clarification).
- All access to Corporate Data should require successful enrolment into the LWETB device management solution.
- Access and storage of Corporate Data is only permitted using approved applications and media (see encryption policy for clarification).
- Access to corporate data may be restricted based on geographical location and may need prior approval from Corporate Services.
- Depending on device capability or security requirements access may be limited to web browser devices.
- Storage of corporate data to local devices may be restricted depending on device capability and/or security requirements.
- Where possible, additional security features relating to corporate applications may be introduced where appropriate, such as additional pin requirements on user timeout.
- Where appropriate, LWETB may exercise its right to wipe Corporate Data from a user's personal device if:

- The device is lost or stolen.
- The employee terminates his/her employment.
- It is determined the device is the source of a data or policy breach, or identified as being infected with a virus or malware which causes a threat to Corporate Data / technical infrastructure security.
- The device does not comply with the standards specified in the current wireless communication standards (802.11 a / b / g / n / ac / ax), as issued by the Institute of Electrical and Electronics Engineers (IEEE).

4. User responsibilities

- When using BYOD outside of the company premises, it must not be left unattended and, if possible, should be physically locked away.
- When using BYOD to access Corporate Data in public places, the User must take care that data cannot be read by unauthorised persons.
- Patches and updates should be installed regularly on BYOD devices.
- Secure Pin / Password / Authentication is required on all BYOD devices used to access / transmit LWETB Corporate Data. A BYOD device must be setup to auto-lock and require Pin / Password / Authentication to unlock if it is idle for ten minutes.
- Users are expected to use their BYOD device in an ethical manner at all times and adhere to LWETB Technology acceptable usage policy at all times / while conducting business.
- Any suspicious activity must be promptly reported to LWETB Data Protection Department by Email.

- It is only permitted to transfer LWETB Corporate data to BYOD devices as per the ICT technical standards outlined in the Encrypt policy.
- Confidential information must be additionally protected according to LWETB Data Classifications and Handling Rules, found at Data Protection Policies and Encryption Policy here.
- Users must notify the Data Protection Officer before the device is being disposed of, sold, or handed to a third-party for maintenance or service;
- Users must ensure all Corporate Data is removed from the device before it is disposed of, sold, or handed to a third-party for maintenance or service.

4.1 User Prohibited Actions

It is not permitted to for users to download Corporate Data to local device storage, or to unauthorised 3rd party cloud storage solutions.

It is not permitted to access Corporate Data where any of the following applies.

- Where the device is shared with anyone else, *e.g.*, the family/household laptop.
- Where the device has been intentionally compromised, *e.g.,* a rooted (Android) or jailbroken (iOS) device.
- If illegal or illicit materials are accessed or stored on the device.
- If there is or has been use of unlicensed / illegally modified software applications.
- Passwords for accounts with access to Corporate Data should not be cached or stored in notes, either in hardcopy or electronically on the device.
- Corporate Data should not be stored locally on a device without file level encryption
- When utilising a connection to unknown Wi-Fi network except when following Remote access for staff policy guidance.

5. Physically Damaged, Lost or Stolen BYOD devices

LWETB will take every precaution to prevent a user's personal data from being lost in the event where a remote wipe of a device must be performed. However, it is the user's responsibility to take additional precautions, such as backing up of personal data on their devices such as email, contacts *etc*. The following conditions apply to physically damaged, lost, or stolen BYOD devices:

- LWETB reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to the LWETB, DPO, Line Manager as soon as possible, and at the latest within 24 hours. Refer to LWETB Data Protection Policies found here .
- The user is personally liable for all costs associated with any loss or theft of a personal device which is, or may have been, used for the purpose of performing employment duties.
- The user is personally liable for all wear and tear or damage to his/her personal device.
- Users are responsible for notifying their mobile network providers immediately upon loss or theft of a mobile phone device

6. Enforcement

Individuals found to be in breach of this policy may be subject to disciplinary action, up to and including dismissal. Should an investigation regarding compliance with this policy determine that there is a case to be answered by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.

7. Policy Review and Continuous Improvement

This document is reviewed every two (2) years in line with best practice, and has been approved by senior management, who are committed to continually improving the protection of all LWETB information assets and the protection of personal data where LWETB is a controller or processor. The date of implementation is the date of Chief Executive approval.

8. Ownership and Approval

OWNER	**DATE**	**SIGNATURE**
Organisation Support & Development Director	Nov 4, 2024	Charlie Mitchell Charlie Mitchell (Nov 4, 2024 16:56 GMT)
AUTHORISED/APPROVED BY	**DATE**	**SIGNATURE**
Chief Executive	Nov 5, 2024	