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

Title	**Bring your own device (BYOD) Policy**
Date	17th August, 2020
Approved By	Chief Executive, LWETB
Noted By	LWETB Board

LWETB
Bring your own device (BYOD) Policy

1. Purpose

The purpose of this policy is to specify the standards, and rules of behaviour for the use of personally-owned smart phones and/or tablets by anyone who accesses LWETB resources and/or services. Access to and continued use is granted on condition that each user reads and follows the policies concerning the use of these resources and/or services.

This policy is intended to protect the security and integrity of LWETB's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

2. Description

This policy applies to all staff, contractors, students, trainees and all who access and use LWETB IT systems using their own personal devices to connect to the LWETB network. BYOD must only allow devices to connect to ether the Guest or Student/Trainee wireless networks.

This policy applies to all devices that connect to the LWETB network or reside on an LWETB site that provide connectivity to endpoint devices including, but not limited to, laptops, desktops, smartphones, and tablets.

LWETB ICT staff or contractors working on behalf of LWETB will respect privacy when working on a personal device and will only request access to the device by technicians to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil or criminal proceedings, or from statutory obligations. This differs from the policy for LWETB-provided equipment and/or services, where employees do not have the right, nor should they have the expectation, of privacy while using equipment and/or services.

3. Definitions

"Acceptable Use", LWETB defines acceptable business use as activities that directly or indirectly support the business of LWETB. LWETB defines acceptable personal use during LWETB working hours as reasonable and limited personal communication or recreation.
"**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

The following activities are considered as unacceptable usage of devices:

- The storing or transmission of illicit materials
- Storing or transmission of proprietary information
- The harassment of others
- Engaging in outside business activities

Employees may use their mobile device to access the following LWETB-owned resources:

- Email
- Calendars
- Contacts
- Internet and hosted services

In order to prevent unauthorised access all devices must:

- Be password protected using the features of the device and a strong password is required to access the LWETB guest network.
- Lock itself with a password or PIN if it's idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- Smartphones and tablets belonging to employees that are for personal use only are not allowed to connect to the network.
- Employees' access to LWETB data is limited and is based on user profiles defined by LWETB ICT Support and automatically enforced.
- Mobile Device Management: all mobile devices must be enrolled on the LWETB MDM system, which provides encryption and hence data security in the event of loss or theft. Before commencing use, users should check that the devices they hold have been enrolled on the MDM system with LWETB ICT Support.
- The employee's device may be remotely wiped if:
    - The device is lost or stolen.
    - The employee terminates his or her employment.
    - ICT Support detects a data or policy breach, a virus or similar threat to the security of LWETB data and technology infrastructure.
    - It fails to abide by the standards specified in the Wireless Communication Standard.
- While LWETB ICT Support will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, but it is the

employee's responsibility to take additional precautions, such as backing up email, contacts, photos etc.

- LWETB reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to ICT Support within 24 hours.
- Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The employee is expected to use his or her devices in an ethical manner at all times and adhere to this policy and to the additional policies outlined at the end of this policy. The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of LWETB and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- LWETB reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

5. Responsibilities

Owner	**Responsibilities**
Director of Organisational Support & Development	Revisions and updates to the policy
LWETB Senior Leadership Team	Review of the Policy
LWETB Chief Executive	Approval of the Policy
LWETB Board	Noting of the Policy
Data Owners	Ensuring implementation of policy.

6. Related Documents /Attachments

- Wireless Devices Policy
- Remote Access Policy
- Password Acceptable Usage Policy
- Asset Protection Policy