City of Dublin Education and Training Board

Bring Your Own Device (BYOD) Policy

Document version	2
Drafted by	ETBI (ICT Group)
Responsibility for this policy in City of Dublin ETB	Director OSD and Head of IT
Reviewed by Senior Leadership Team (SLT)	12 October 2021
Approved by Chief Executive	12 October 2021
Noted by Board	21 October 2021
To be reviewed	1 year from date of approval by CE

Contents

1 Introduction 3

1.1 Purpose of this Document 3
1.2 Scope and Constraints 3
1.3 Definitions 3
1.4 Policy Review, Approval and Continuous Improvement 3

2 BYOD Policy Overview 4

3 Requirements for BYOD devices 4

3.1 ICT technical standards 4
3.2 User responsibilities 5
3.3 User Prohibited Actions 5

4 Lost or Stolen BYOD devices 6

5 Enforcement 6

1 Introduction

1.1 Purpose of this Document

The BYOD policy is defined in the City of Dublin ETB ICT Framework Policy and should be read in conjunction with all other IT policies to ensure that required security standards are adhered to. This policy is intended to protect the security and integrity of the City of Dublin ETB's Corporate Data and technology infrastructure. It outlines the IT Department-set standards and also the user's responsibilities to keep corporate data safe where City of Dublin ETB consents to employees choosing to use personal devices for work purposes or where an employee consents to City of Dublin ETB's 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 City of Dublin ETB corporate data to or from a device not registered in the organisation's device management solution or personal device. This policy is effective as of the issue date and does not expire unless superseded by another policy.

By connecting to City of Dublin ETB 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 City of Dublin ETB infrastructure.

1.3 Definitions

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

1.4 Policy Review, Approval and Continuous Improvement

In line with best practice, this policy has been approved by senior management, who is committed to continually improving the protection of all City of Dublin ETB information assets and the protection of personal data where City of Dublin ETB is a controller or processor. This document will be reviewed annually by senior management, to ensure alignment to appropriate risk management requirements and best practice for the management of ICT devices within City of Dublin ETB.

2 BYOD Policy Overview

This policy outlines the standards required and upheld by the IT Department as well as the responsibilities of users who wish to access City of Dublin ETB Corporate Data from their own personal devices, or any device not registered within the organisation's device management platform.

City of Dublin ETB users/employees must agree to the terms and conditions set forth in this policy before connecting, or continuing to connect, their devices to the organisation's technology infrastructure.

City of Dublin ETB will respect the privacy of personal devices and may only request access to the device by the IT Department 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 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);
- 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 the IT Department;
- Depending on device capability or security requirements access may be limited to web browser only for some or all BYOD 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, City of Dublin ETB 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;

3.2 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 must be installed regularly on BYOD devices;
- Secure Password is required on all BYOD devices used to access / transmit City of Dublin ETB Corporate Data. A BYOD device must be setup to auto-lock and require Password to unlock, if it is idle for fifteen minutes;
- Users are expected to use their BYOD device in an ethical manner at all times and adhere to City of Dublin ETB**'s** IT Usage Policy while conducting business;
- Any suspicious activity must be promptly reported to City of Dublin ETB's IT Department;
- It is only permitted to transfer City of Dublin ETB Corporate data to BYOD devices as per the ICT technical standards outlined in the Encryption policy.
- Users must notify the IT Department before the device is being disposed of or sold;
- Users must ensure all Corporate Data is removed from the device before it is disposed of or sold.

3.3 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;
- Where passwords for accounts with access to Corporate Data have been cached or are stored in notes, either in hardcopy or electronically on the device.
- Where Corporate Data will 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)

4 Lost or Stolen BYOD devices

City of Dublin ETB 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 lost or stolen BYOD devices:

- City of Dublin ETB reserves the right to disconnect devices or disable services without notification;
- Lost or stolen devices must be reported to the City of Dublin ETB’s IT Department as soon as possible, and at the latest within 24 hours.
- 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.

5 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 answer by a User, the matter will be referred to the appropriate stage of the relevant disciplinary procedure as appropriate to that User.