Mobile Phones Acquisition and Acceptable Usage Policy for ETB Business Plan Users

V1.15 September 2023

Policy/ Document No: PL/016	Version No: V1.15 September 2023

Table of Contents

1 Scope

Dublin and Dun Laoghaire ETB (DDLETB) staff availing of the DDLETB Mobile Business Plan must abide by this policy. Mobile business users are any users that receive a business mobile phone or allowance. Staff are expected to use common sense and to conduct themselves in a manner which is appropriate to the execution of their duties in the workplace.

This policy should be read in conjunction with other existing DDLETB policies.

These policies are available on the DDLETB website.

2 ICT Technical Standards

- All access to DDLETB data is made available using encrypted communications standards only
- All access to DDLETB Data requires the use of Multi-Factor Authentication (MFA)
- All access to DDLETB Data requires successful enrolment into the DDLETB device management solutions
- Access and storage of DDLETB Data is only permitted using approved applications and media
- Access to DDLETB data may be restricted based on geographical location and may need prior approval from the DDLETB Information Communications Technology Department, hereafter collectively referred to as the ICT Department.
- Storage of DDLETB data to local DDLETB devices may be restricted depending on device capability and/or security requirements. DDLETB data must be saved to DDLETB servers or to DDLETB cloud infrastructure.
- Where possible, additional security features relating to DDLETB applications may be introduced where appropriate
- Where appropriate, the ICT Department may exercise its right to wipe DDLETB Data from a DDLETB device if:
    - The device is lost or stolen;
    - The employee terminates his/her employment
    - The employee retires or resigns
    - 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 DDLETB Data / ICT infrastructure security;
- There ICT Department will provide advice where mobile connectivity is required for Building Management Systems, alarms, lifts etc.
- The ICT Department will from time-to-time issue detailed technical guidelines where appropriate
    - The Equipment Loan Agreement has been issued in relation to the provision of DDLETB devices

3 User responsibilities

- When using a DDLETB device outside of a school, college, centre or FET Service, it must not be left unattended and, if possible, should be physically locked away;
- When using a DDLETB device to access DDLETB 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 a DDLETB device;
- Secure Pin / Password / Authentication is required on all DDLETB devices used to access / transmit DDLETB Data. A DDLETB 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 a DDLETB device in an ethical manner at all times and adhere to DDLETB policies at all times
- Any suspicious activity must be promptly reported to the ICT Department
- It is only permitted to transfer DDLETB data to a DDLETB device
- Users must notify the ICT Department before any DDLETB device is being disposed of, sold, or handed to a third-party for maintenance or service;
- Users must ensure all DDLETB Data is removed from a DDLETB device before it is disposed of, sold, or handed to a third-party for maintenance or service.
- Users must be mindful of DDLETB obligations when subscribing to services or applications including, but not limited to security, data protection and procurement
- For mobile devices provided by DDLETB you must safeguard all documentation associated with the equipment and store it in a safe place. (The documentation forms part of the equipment inventory and must be released with the unit for termination of contracts, equipment upgrade etc.).
- Should a device be lost or stolen, the user should contact the ICT Department. The loss must also be reported to the Data Protection Officer at dataprotection@ddletb.ie.

4 User Prohibited Actions

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

It is not permitted to access DDLETB Data where any of the following applies;

- Where the device is shared with anyone else
- 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;
- When utilising a connection to unknown Wi-Fi network. (except when following Remote access for staff policy guidance)
- In addition;
- Users must not use a DDLETB Microsoft 365 account when registering for personal applications, services or subscriptions
- Users must not use DDLETB Microsoft 365 credentials for personal applications, services or subscriptions
- Users must not forward emails (automatically or otherwise) to non DDLETB email systems
- Users must not synchronise DDLETB data to personal Microsoft, Google, Apple, Adobe or other such non -approved email/data storage systems
- Users must not use personal email addresses, Apple ID or other such non-approved methods to login into DDLETB devices, applications or cloud systems.
- Users must not use personal email addresses for DDLETB business

5 General Device Usage Regulations and Guidelines

5.1 Usage

Access to mobile business plan is intended for ETB's purposes only including, but not limited to calls, texts, communications via apps. While reasonable making and taking of personal calls is not strictly prohibited, staff are encouraged to keep this to a minimum level during working hours. DDLETB reserves the right to monitor use on the mobile business plan.

5.2 Accountability

Mobile business plan usage should be able to withstand public scrutiny and/or disclosure. Staff should not use their mobile phones in a way that could defame, harass, bully, abuse or offend individuals, the ETB or organisations.

DDLETB reserves the right to audit any or all ETB funded mobile phone usage. Staff may be called upon to explain their use of the ETB funded mobile business plan. The recording of images/pictures on mobile phones during working hours is not permitted unless part of your duties.

5.3 Courtesy

As a matter of professional courtesy, we advise mobile phone users to either turn off their phone or divert it to voicemail or another number, or set the phone into "silent mode" during meetings, training courses, seminars etc. In exceptional circumstances, where it becomes necessary to take a business call, it is courteous to inform colleagues that an urgent call is expected, and then take steps to minimise the call impact.

5.4 Use of Mobile Phones whilst driving

It is illegal to hold or use mobile phones whilst driving. DDLETB does not accept legal liability for any penalty incurred by staff who infringe upon the law with regard to the use of mobile phones. Users are recommend to familiarise themselves with the Road Safety Authority (RSA) campaigns on mobile phones and distractions

5.5 Voice-Mail

Your Voicemail should be personalised with the following message:-
"Hello - you have reached (your name), DDLETB's voice mail, I am unable to take your call at present however if you leave your name and number and a brief message, I will contact you as soon as I can. Thank you."

5.6 Legislation

Staff are subject to all legislation regulating the use of the ETB's communication technology. Staff must not store, download, upload, circulate or otherwise distribute material containing:

- Any derogatory comment regarding gender, material status, family status, sexual orientation, religious or political belief, age, disability, race or membership of the travelling community or other categories pursuant to applicable law.
- Any material of a pornographic nature.
- Any material of a paedophilic nature.
- Material containing offensive or foul language.
- Any content prohibited by law.

If a staff member receives any offensive, unpleasant, harassing or intimidating messages he/she should:

- Bring it to the attention of his/her line manager, the Head of HR or Head of ICT;
- Inform the sender that such images are offensive and that they should refrain from sending such images in future; and

5.7 Mobile Phone types

All DDLETB mobile phone devices and associated equipment must be purchased in line with DDLETB procurement contracts. The contact details for all current contacted mobile phone business plan service providers can be obtained from the ICT Department, DDLETB Head Office, Tuansgate, Dublin 24.

Only mobile phone devices which have been purchased in line with DDLETB procurement contracts through the ICT Department approved channels will be allowed connection to the DDLETB network.

All DDLETB provided mobile phone devices, associated equipment and mobile phone numbers remain the property of the DDLETB.

5.8 Software Ownership

All software which is provided by DDLETB to a user is licensed and owned by the DDLETB and may not be downloaded, stored elsewhere or transferred to another individual by any employee of the DDLETB.

Under no circumstances should software be downloaded from the Internet or installed from any other source and used on the DDLETB's devices without the prior permission of the ICT Department. Any breach of these requirements may result in disciplinary action.

5.9 Line manager Responsibilities

The Line Manager must

- Ensure ETB mobile business plans are only issued to staff members who require a mobile phone for business reasons.
- Ensure that the staff to whom it is allocated only uses the equipment approved by ICT Department.
- Ensure that records regarding mobile phones are kept up to date i.e. current user and cost centre, asset register etc.

5.10 Allocation of Mobile Phones

5.10.1 Mobile phones are only issued to staff on the basis of "Business need." A business need is defined as follows:

- Staff whose job entails significant working hours spent travelling away from their main location of work; and
- Staff who agree with their manager that they must be contactable at any time.
- Staff who are required to be contactable outside of normal working hours, such as senior management and those responsible for security at sites, or those employees required to take action in the event of an emergency.
- And any other reason deemed appropriate from time to time.

5.10.2 Any requests to be included in the ETB Mobile Business Plan through this policy, staff must complete the ETB's mobile and portable modem device business user official request application form and this form must be signed by their line manager. The completed application request form should then be submitted to the Head of HR.

5.10.3 The Head of Organisation Services and HR shall assess:

- whether an employee's work necessitates a business user mobile phone in the discharge of their duties and, if approved,
- the type of mobile and/or portable modem device if required.

5.10.4 In the event of HR approval, ICT will contact our service provider to arrange for a business user account to be set-up in the staff member's name. ICT shall advise the staff member of detail of delivery or collection.

5.10.5 DDLETB's contract with the mobile provider is to facilitate this arrangement.

5.10.6 The mobile phone contract shall be between the staff member and the service provider. DDLETB is not a party to this contract.

5.11 Billing/Allowance

The staff member will be paid an allowance each month equal to the amount of the flat rate charges. (which is negotiated by DDLETB with the service provider).

- The staff member shall pay the full amount of the bill to the service provider. In the event that there are no calls outside the scope of the tender with the provider, the amount of this payment will be equal to the amount of the allowance above. If there is a situation where the individual is required to pay for a work related call i.e. where a call is made in furtherance of a work related issue that is not comprehended to be within the flat rate charge, the staff member shall reclaim this amount through the Sun System.

- Billing will be borne by the staff member and work-related charges shall be recouped from the ETB via the Sun System.

5.12 Call Charges

All normal calls and texts placed and received within ROI will be free (inclusive of the prevailing rate). All business-calls will be refunded through the Sun System. All non-normal calls and texts i.e. Premium rate calls or premium texts (11811 transfer calls, or calls to 1530, 1550 numbers etc.) will not be refunded through the Sun System as you are personally liable for these call costs.

5.13 Termination of Contract

When the staff member's employment with the ETB cease, he/she must return any devices provided by DDLETB to ICT. The staff member should advise the service provider. Permission must be requested from the ICT Department to retain the number.

5.14 Security

To ensure DDLETB compliance with data protection and security of data only authorised DDLETB business users are permitted to have access to work email on DDLETB mobile handsets.

5.15 Roaming

If enabled the cost will be borne by the individual unless it is a business call which should be claimed on the Sun System. Users should note that data allowances while roaming are reduced when compared to standard allowance.

5.16 Access to DDLETB tariffs

If a staff member ceases to be an employee of DDLETB, (contract of employment comes to an end, employee resigns or retires) access to the DDLETB tariffs will cease and the staff member will revert to the standard consumer tariffs with the service provider.

5.17 Infringements of Policy

Failure to comply with the policy and guidelines outlined above may result in:

- The withdrawal of access to DDLETB devices and systems from the user(s) involved
- Initiation of disciplinary procedures and disciplinary action, up and to including dismissal.
- Serious breaches of the policy may result in initiation of criminal or civil proceedings.

5.18 Bring Your Own Device (BYOD)

BYOD is not permitted within the DDLETB.

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 DDLETB infrastructure.

For clarity, a parent/guardian owned device, managed by a DDLETB Mobile Device Management system in a 1:1 environment is not regarded as a BYOD device.

APPENDIX A Definitions used throughout the listed policies

- **DDLETB Data –** means any and all **data** maintained by 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**- The term device refers to any desktop, laptop, tablet or similar hardware used to connect to DDLETB ICT infrastructure

- **Device Management Solution** - is a type of management or security technology that enables IT administrators to monitor, manage and secure DDLETB devices that run across multiple operating systems;

- **Encryption** – the process of converting information so that it cannot be read by unauthorised people;

- **Information** - The term information refers to knowledge which may be stored in any form, whether printed or in electronic form;

- **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;

- **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, documented and approved by appropriate management 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;

- **Technology Infrastructure –** All computing, connectivity and cloud-hosted technology owned or managed by DDLETB and its contracted third parties;

- **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.

- **Remote Access -** refers to the use and administration of the remote working environment utilised by DDLETB to facilitate the processing of DDLETB Data by employees.

APPENDIX B Relevant statues

DDLETB 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
  DDLETB has a number of 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 DDLETB

- Safety, Health and Welfare at Work Acts

- Copyright and Related Rights Acts
  The copying of software or documents which are copyrighted is an offence. DDLETB has a policy whereby only licensed media are used within the organisation.

- 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.

- Other legislation may include
    - Employment Equality Acts, 1998 to 2015
    - Equal Status Act, 2000 and 2012
    - General Data Protection Regulations GDPR
    - The Education and Training Boards Act, 2013
    - The Companies Acts 1963 - 2001
    - Freedom of Information Legislation 2014
    - National Archives Act 1986

    - 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)

APPENDIX C Business User Mobile Phone Application Form

Application to: **HR Manager**

From: _____ Date: _____

Staff Member

I wish to apply for a Business Mobile Phone **New** ☐ **Upgrade** ☐

Brief description of your duties /role:	
Reasons why you deem you need the above in the performance of your role:	

Line Manager: _____

Date: _____

----------***FOR HEAD OFFICE USE ONLY*** ----------

On the basis of the application above and a review of the role and duties we deem the employee (*tick appropriate*)

Merits application ☐ Does not merit application. ☐

_____ _____

Head of Organisational Services HR Manager

Date: _____

APPENDIX D Mobile Phone Business Plan Acceptance (with Handset)

By my signature below, I acknowledge receipt of the following equipment in good working condition. Additionally, my signature below indicates that I have read and understand the DDLETB Mobile Phone Business Plan Policy and agree to the conditions of this policy.

Handset Details:

Make : _____

Model:

IMEI Number:

Mobile Phone Number:

Printed Name of Phone User

Signature

Position/Title

School/Centre Location:

Date

Mobile Provider

On behalf of Three Ireland, I confirm the above details are correct.

_____Signature

APPENDIX E Mobile Phone Business Plan Acceptance (without Handset)

My signature below indicates that I have read and understand the DDLETB Mobile Phone Business Plan Policy and agree to the conditions of this policy.

Mobile Phone Number:

Printed Name of Phone User

Signature

Position/Title

School/Centre Location:

Date

Mobile Provider

On behalf of Three Ireland, I confirm the above details are correct.

_____

Signature