ddletb

Bord Oideachais agus Oiliúna Átha Cliath agus Dhún Laoghaire
Dublin and Dún Laoghaire Education and Training Board

INFORMATION & COMMUNICATION TECHNOLOGY (ICT) ACCEPTABLE USAGE POLICY

V1.6 July 2023

Policy/ Document No: PL/016	Version No: V1.6 July 2023
Previous versions: V1.5 November 2018	Effective Date: July 2023
Board App/Noting Sept. 2023	Review Date: 14/07/2023

Table of Contents

1. Scope

This policy applies to any person authorised to have access to Dublin & Dun Laoghaire Education & Training Board (*DDLETB*) information systems. This includes but is not limited to *DDLETB* employees (managers and staff), contractors to *DDLETB* and consultants engaged by *DDLETB* hereafter collectively referred to as users for the purpose of this policy.

This policy applies to all ICT Infrastructure & Services provided by *DDLETB* including, but not limited to internet/cloud services, e-mail, desktop computers, laptops and tablet devices, digital cameras, phone infrastructure (including desktop, soft and smartphones), applications and cloud systems. It is the responsibility of users to ensure that all such tools are used in accordance with this policy.

All users are expected to use best practice and to conduct themselves in a manner, which is appropriate to the execution of duties in the workplace. Breaches of this policy may result in personal liability of users and/or vicarious liability on behalf of *DDLETB* under relevant statutes including, but not limited to those listed in Appendix B.

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;
- The ICT Department will from time to time issue detailed technical guidelines related to DDLETB Technology Infrastructure
- The ICT Department will apply the principle of least privilege to access controls in order to ensure that users do not operate with elevated privileges where these are not required

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
- 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, *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;
- 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 store DDLETB data to local Desktop or My Documents folders as such locations are not secured by DDLETB backups
- 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, personal Apple ID or other such non-approved methods to login into DDLETB devices, applications or cloud systems.
- Users must not create local logins that bypass or replace those created by the ICT Department.
- Users must not use personal email addresses for DDLETB business
- Users must not introduce Shadow ICT into the DDLETB Technology Infrastructure

5. General Device Usage Regulations and Guidelines

5.1 Contents

All electronic content created or received using equipment or services provided by *DDLETB* will be regarded as the property of *DDLETB*.

5.2 Equipment and Resources

All equipment provided by *DDLETB* for use by staff remains the property of the *DDLETB*. Employees must not remove any such equipment including but not limited to desktop computers, laptops, tablets, mobile telephones, etc. from the *DDLETB*'s premises without prior authorisation from the line manager. If equipment is removed, it must be kept in a secure environment by the user.

It is the responsibility of users to return equipment to the DDLETB at the end of employment contract, retirement, resignation etc.

It is the user's responsibility to be informed of the correct operating procedures for DDLETB devices or applications. A user who is uncertain as to the correct procedure in any situation should obtain clarification from the ICT Department before proceeding.

Users must not engage in conduct that interferes with other's use of shared ICT resources and/or the activities of other users.

5.3 Security and Passwords

Users must not utilise any other person's access rights or attempt to gain access to resources or data. In exceptional circumstances where access is required, it must be requested in writing by the Head of the Dept. to the Head of I.C.T. Users must not attempt to bypass or probe any security mechanisms governing access to devices or applications.

No staff member may misrepresent himself / herself as another individual. This includes using another staff member's username and password.

Passwords must remain confidential to each user and must not be relayed to any other person. The ICT Department may provide the option to alter any passwords as necessary. Each user carries sole responsibility for security access to his/her computer, laptop or any other electronic device.

5.4Software 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/cloud services

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.

5.5 *Confidentiality*

Users must maintain confidentiality while carrying out their duties and while on *DDLETB* business.

5.6 *Privacy*

It should be understood that *DDLETB* does not provide users with a guarantee or to the right to privacy or confidentiality in connection with the use of any technology and users should have no expectation of privacy in the use of the *DDLETB*'s ICT resources.

5.7 *Monitoring Policy*

DDLETB reserves the right and intent to monitor ICT infrastructure including, but not limited to, e-mail content and Internet/Cloud Services usage to ensure technology is being used properly and to protect *DDLETB* and its employees from liability, including, but not limited to equality, data protection, pornography and copyright legislation. This does not constitute infringement of any individual rights to personal privacy under Data Protection and the GDPR. Appendix B contains examples of relevant statutes.

Monitoring may be carried out on all Electronic Data including all Web site, Desktop and device content. This list is not exhaustive. Monitoring developments may change over time. In addition, *DDLETB* may monitor all devices for inappropriate images and content.

Mobile Device Management (MDM) software is mandatory and installed on all devices including laptops, tablets etc.

5.8 *Legal Implications of Storing Electronic Data*

All information held in electronic format is subject to legislative requirements, as is information held in paper format. These requirements include but are not exclusive to Copyright, Data Protection and Freedom of Information Legislation and the liabilities which may result from breaches of such legislation. Appendix B contains examples of relevant statutes.

Personal information should contain only information relevant to the individual and to the purpose for which it is being stored. Data must not be used for any other purpose. This data must be maintained in an accurate format and must be altered if the user/Board becomes aware of inaccuracies.

It is an offence to alter or falsify documents in an electronic format or paper / hard copy format. Care must be taken when forwarding or sending information which has been received from a third party or which is specific to another organisation.

Employees should be aware that merely deleting information may not remove it from the system and deleted material may still be reviewed by the employer and / or disclosed to third parties.

5.9 *Material of obscene or offensive nature*

Users are subject to all legislation regulating the use of *DDLETB*'s ICT resources. Users 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 user receives or observes any such material, the user should bring it to the attention of their line manager, the ICT Manager or the HR Manager;

5.10 Security

Ransomware and Viruses can enter an organisation a number of different ways:

- Unscanned digital storage media (e.g. CDs, DVDs, floppy disks, USB memory sticks) being brought into the organisation.
- E-mails or attachments
- Downloaded data from the Internet/Cloud Services.

Users with DDLETB devices must be familiar with and comply with the *DDLETB*'s procedures governing usage of USB's, SD Cards, CD's and other software. It is the personal responsibility of each user to take precautions to ensure that viruses are not introduced into any *DDLETB* devices or systems with which they come into contact.

No user may interfere with or disable the Security/Anti-Virus software installed on their device. Any virus or security incidents, virus error or security messages must be reported promptly to the ICT Department.

6. Microsoft 365 Infrastructure (including Email, Teams etc.)

Users are provided with a Microsoft 365 account to allow communications between staff, learners and between the *DDLETB* and its clients and suppliers.

All email communications must be done using Microsoft 365 infrastructure only. While email brings many benefits to *DDLETB* in terms of its communications internally and externally, it also brings risks to the organisation, particularly where employees use it outside of their *DDLETB* roles.

All online meetings originating within DDLETB must use Microsoft 365 infrastructure only.

Every employee has a responsibility to maintain *DDLETB*'s image, to use electronic resources in a productive manner and to avoid placing *DDLETB* at risk for legal liability based on their use. It should be remembered that the contents of e-mail are considered as official records for the purpose of legislation such as Freedom of Information Act, National Archives Act, and Data Protection.

6.1 Risks Associated with E-Mails

- Messages can carry ransomware viruses and/or links to same that may be seriously damaging to the *DDLETB*'s systems
- E-Mail attachments may belong to others and there may be copyright implications in sending or receiving them without permission.
- It has become increasingly easy for messages to go to persons other than the intended recipient and if confidential or commercially sensitive, this could be breaching *DDLETB*'s security and confidentiality and more generally data protection obligations
- E-mail is speedy and, as such, messages written in haste or written carelessly are sent instantly and without the opportunity to check or rephrase. This could give rise to legal liability on the part of *DDLETB*.
- An e-mail message may legally bind *DDLETB* contractually in certain instances without the proper authority being obtained internally.
- E-mails should be regarded as potentially public information, which carries a heightened risk of legal liability for the sender, the recipient and the organisations for which they work.
- E-mails may contains phishing links, seek to appear as legitimate internal or external contacts and seek to initiate frauds such as invoice redirection.

If in doubt about an E-mail, please contact the ICT Department.

6.2 Rules for E-Mail Use

The content of any e-mail must be in a similar style to that of any written communication such as a letter or report as they have the same legal standing. It is important that e-mails are treated in the same manner as any other written form of communication in terms of punctuation, accuracy, brevity and confidentiality. Similarly, any written, stored or forwarded and disseminated information must adhere to the guidelines within the

Data Protection and the Employment Equality legislation and in accordance with the equality policy of *DDLETB*. Appendix B contains examples of relevant statutes.

In order to avoid or reduce the risks inherent in the use of e-mail within *DDLETB*, the following rules must be complied with:

- The *DDLETB*'s corporate signature must appear at the end of every e-mail sent from your *DDLETB* address to an external address.

- The *DDLETB*'s school, college, centre or FET Service name is included in the address of all staff members and is visible to all mail recipients. This reflects on the image and reputation of the organisation, therefore, e-mail messages must be appropriate and professional.

- Correct spelling and punctuation should be maintained in all communications.

- DDLETB e-mail is provided for business purposes.

- An e-mail should be regarded as a written formal letter, the recipients of which may be much more numerous than the sender intended. Therefore any defamatory or careless remarks can have serious consequences, as can any indirect innuendo. The use of lewd, indecent, obscene, sexist, racist, harassing or other inappropriate remarks whether in written form, cartoon form, video, audio or otherwise is forbidden.

- E-mails must not contain content which may discriminate on grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community.

- Distribution lists may only be used in connection with *DDLETB* business.

- Documents prepared internally for the public or for clients may be attached via the e-mail. However, excerpts from reports other than our own may be in breach of copyright and the author's consent should be obtained particularly where the excerpt is taken out of its original context. Information received from a customer should not be released to another customer without prior consent of the original sender. If in doubt, consult your manager.

- Do not subscribe to apps or cloud services or other contracts on behalf of *DDLETB* unless you have express Board approval to do so.

- If you receive any offensive, unpleasant, discriminatory, harassing or intimidating messages via the e-mail system you must immediately inform your manager, the ICT Manager or the HR manager.

- Chain mails or unsuitable information must not be forwarded internally or externally.

- *DDLETB* reserves and intends to exercise the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose or where it deems necessary.

- Notwithstanding *DDLETB*'s right to retrieve and read any E-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorised to retrieve or read any e-mail messages that are not sent to them. However, the confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message.

- Users must not register with an app or cloud service, without prior permission from their Line Manager and from the ICT Manager. This is in order to avoid the release of confidential *DDLETB* information to third parties.

- Users must familiarise themselves with the appropriate use of email features such as bcc and encryption options

7. The Internet/Cloud Services

Access to the Internet / cloud services is provided to staff as necessary solely for the purpose of conducting the *DDLETB*'s business. All information and uploaded content on the intranet or loud services is the property of *DDLETB*.

7.1 Rules for Internet/Cloud Services use

- The *DDLETB*'s Internet/Cloud Services connections are intended for activities that either support the *DDLETB*'s business or the professional development of employees.

- Internet/Cloud Services usage may be monitored on a systematic basis and as deemed necessary by *DDLETB*.

- Unauthorised downloading of any software programmes or other material is forbidden.

- It is a disciplinary offence to access, download, save, circulate or transmit any racist, defamatory or other inappropriate materials or materials that may discriminate on the grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community. This rule will be strictly enforced and is viewed very seriously with potential criminal liabilities arising therefrom.

- It is a disciplinary offence to access, download, save, circulate or transmit any indecent, obscene, child pornographic or adult pornographic material.

- If user is downloading pornographic images within view of other user(s) or forwarding those images to user(s), this may result in harassment or sexual harassment by offended parties. Such incidents must be reported to the relevant *DDLETB* manager. Apart from any potential offence caused and the inappropriateness of such activity, *DDLETB* may be vicariously liable for any claims arising from such behaviour.

- Because of the serious criminal implications of accessing child pornography, any employee found to be accessing such information may be summarily dismissed and for any user, the matter referred to An Garda Síochána. Furthermore, should an employee be prosecuted under the Child Trafficking and Pornography Act, 1998, by engaging in such activities outside the remit of the workplace, *DDLETB* may find it fitting to invoke disciplinary action.

- The Internet/Cloud Services must not be used to pay for, advertise, participate in or otherwise support unauthorised or illegal activities.

- The Internet/Cloud Services must not be used to provide lists or information about the organisation to others and/or to send classified information without prior written approval.

8. Voice Infrastructure

Access to desk, soft or mobile phones is intended for *DDLETB* purposes only. While reasonable making and taking personal calls is not strictly prohibited, staff are encouraged to keep this to a minimum level. *DDLETB* reserves the right to monitor the use of the voice infrastructure.

Some mobile phones are provided to staff members for *DDLETB* business. Personal calls from such phones are permitted once payment is made by the staff member. For more specific information see *DDLETB*'s Mobile Phones Usage Policy.

During office hours, the taking and/or making of calls on personal mobiles is not strictly prohibited however, staff are encouraged to keep such calls to a minimum.

9. Other Electronic Tools

Other electronic equipment (e.g. smart TVs, digital signage, printers, cameras, fax machines etc.) remain the property of *DDLETB* and as such must be treated with care and used only for *DDLETB* purposes. Abuse of equipment for personal use or gain may result in the use of the disciplinary procedures and in disciplinary action.

10. Plagiarism

Users should not plagiarise (or use as their own, without citing the original creator) content, including words or images from the Internet/Cloud Services. Users should not misrepresent themselves as the author or creator of something found on-line. Research conducted via the Internet/Cloud Services should be appropriately cited, giving credit to the original author.

11. Social Media

DDLETB recognises the presence and value of social media tools which can facilitate communication, learning and collaboration. When using these tools, users are expected to communicate with the same appropriate and professional conduct online as offline.

Users should consider rules governing copyright, intellectual property and confidentiality before posting to social media.

Users should be mindful of their privacy settings and postings on personal social platforms. Employees should note that the use of social media in a work setting is subject to the same guidelines and rules as previously outlined in this policy. For more specific information see *DDLETB*'s Social Media Policy.

12. Removable Media

Removable media such as CD, DVD, USB drive or SD cards etc. must not be used to store & transport DDLETB data.

If in doubt about storage of data, please contact the ICT Department.

13. Encryption

All DDLETB data stored on *DDLETB* devices must be protected by encryption software. It is the responsibility of the staff member to ensure that the data is encrypted and the encryption software is up to date.

If in doubt about encryption, please contact the ICT Department.

14. 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.

15. Remote Access

This section covers two aspects of remote access:

1. Internal User access (remote working or remote access to systems)
2. External User access on an AD-hoc basis and in accordance with agreed SLA.

15.1 Remote Working

If approved for remote working, DDLETB will supply staff with ICT equipment to enable them to work remotely.

Staff are required to sign a loan agreement before receiving such equipment and the equipment must be returned when the need for remote working no longer applies, employment contract ends or with retirement.

Equipment remains the property of DDLTB at all times.

For further details, please refer to the DDLETB Remote Working Policy

15.2 ICT Technical Standards

1. Remote access for DDLETB users must be approved by the ICT Department.
2. Configuration standards & usage protocols must be agreed with the ICT Dept. for all remote access system components;

15.3 Third Parties' Responsibilities

1. Remote access technologies used to access DDLETB technology infrastructure by third parties must be configured to automatically disconnect sessions after 10 minutes of inactivity.
2. Configuration standards must be developed for all remote access system components
    a) These standards must address all known security vulnerabilities and be consistent with industry-accepted system hardening standards;
    b) System configuration standards must be updated as new vulnerability issues are identified;
    c) System configuration standards must be applied when new systems are configured and verified as being in place before a system is utilized in the DDLETB technology infrastructure.
3. Maintenance shall only be performed as agreed with DDLETB
4. Where permitted, remote access for supplier maintenance or diagnostics purposes will be strictly controlled to protect the security of the system.
5. Security controls must be agreed and defined in a contract with the third party and must include an agreed method of access.
6. Any suspicious activity must be promptly reported to the DDLETB ICT Department.

   All remote access to corporate data by third party suppliers must be agreed as part of a data sharing agreement by DDLETB
7. Where temporary remote access is required by a third party, it must be granted as follows:
    a) Access must be requested prior to attempting connnection;
    b) Must be deactivated or disabled immediately after each use;
8. Third party organisations (customer or support organisation), shall only be provided with remote access on a temporary basis.

15.4 User Responsibilities

1. Only ICT department approved secure remote access technologies, such as LOGMEIN may be used when accessing DDLETB systems.
2. Remote access tools that establish outbound and always-up connections are not permitted unless ICT Department approved [*e.g.* VNC, Team Viewer and Logmein *etc*].
3. Access to company data must only be carried out over secure sessions using approved encryption.
4. Remote users must be registered and authorised prior to using the service allowing connection to DDLETB Data.

5. The use of DDLETB remote access solution must require Multi Factor Authentication .
6. Any suspicious activity must be promptly reported to ICT Department.
7. Remote credentials (including any secure fob) must not be shared with anyone.

16. 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.

APPENDIX A Definitions used throughout the listed policies

- **BYOD – "Bring Your Own Device" -** the practice of allowing the employees of an organisation to use their own computers, smartphones, or other devices for the purpose of performing employment duties;

- **DDLETB Data –** means any and all **data** maintained by **DDLETB** 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;

- **HTTPS** - Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer;

- **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;

- **Shadow ICT** – refers to the use of ICT-related hardware or software by any DDLETB location, department or user, without the knowledge of the ICT Department. Shadow ICT can encompass cloud services, software, and hardware. The use of Shadow ICT may introduce security , governance and related risks to DDLETB data and technology infrastructure.

- **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
  - 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
  - National Archives Act

  - 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)