

INFORMATION & COMMUNICATION TECHNOLOGY (ICT) ACCEPTABLE USAGE POLICY

V1.5 November 2017

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

Table of Contents

1. Scope	3
2. General Computer Usage Regulations and Guidelines	3
2.1 Contents.....	3
2.2 Equipment and Resources	4
2.3 Security and Passwords.....	4
2.4 Software Ownership	4
2.5 Confidentiality.....	4
2.6 Privacy.....	5
2.7 Monitoring Policy	5
2.8 Legal Implications of Storing Electronic Data	5
2.9 Material of obscene or offensive nature	5
2.10 Virus Protection.....	6
3. E-Mail	6
3.1 Risks Associated with E-Mails	7
3.2 Rules for E-Mail Use	7
4. The Internet/Intranet.....	9
4.1 Rules for Internet use	9
5. Telephone Usage	10
6. Other Electronic Tools.....	10
7. Plagiarism.....	11
8. Social Media.....	11
9. Removable Media	11
10. Infringements of Policy	11
11. Encryption	11

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

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, 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 electronic communications systems provided by **DDLETB** including, but not limited to internet, intranet, e-mail, personal computers, laptops and tablet devices, digital cameras, Telecommunication systems and devices. It is the responsibility of both management and staff of **DDLETB** to ensure that all such tools are used in accordance with this policy.

All users are expected to use common sense 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 many enactments including, but not limited to the following:

- Employment Equality Acts, [1998](#)
- Equal Status Act, [2000](#) and [2012](#)
- Data Protection Act [1988 and 2003](#)
- General Data Protection Regulations [GDPR](#)
- The Education and Training Boards Act, [2013](#)
- The Companies Acts [1963 - 2001](#)
- Copyright and Related Rights Act [2000](#), [2004](#) and [2007](#)
- Child Trafficking and Pornography Act 1990 [1998](#) and [2004](#)

Other documentation that is relevant to this policy includes **DDLETB**'s policies on:

- Social Media
- Mobile Phone
- Grievance and Discipline
- Dignity and Respect at Work - Equality and Diversity
- Harassment and Sexual Harassment
- Bullying in the workplace
- Leavers and Transfers Procedures

2. General Computer Usage Regulations and Guidelines

2.1 Contents

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

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

2.2 *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 computers, laptops, 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 user's responsibility to be informed of the correct operating procedures for the computer resources or products used. A user who is uncertain as to the correct procedure in any situation should obtain clarification before proceeding.

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

2.3 *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 the computer systems.

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.

2.4 *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 machines without the prior permission of the ICT Development & Management Officer. Any breach of these requirements may result in disciplinary action.

2.5 *Confidentiality*

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

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

2.6 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.

2.7 Monitoring Policy

DDLETB reserves the right and intent to monitor e-mail content and Internet usage to ensure technology is being used properly and to protect **DDLETB** and its employees from liability under 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.

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

2.8 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.

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.

2.9 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, marital 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.

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

- Any material of a pornographic nature.
- Any material of a paedophilic nature.
- Material containing offensive or foul language.
- Any content prohibited by law.

If an employee receives any offensive, unpleasant, harassing or intimidating messages via e-mail or other computer sources the employee should bring it to the attention of their line manager, the ICT Manager or the HR Manager;

2.10 Virus Protection

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.

Individuals using electronic information 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 individual to take precautions to ensure that viruses are not introduced into any **DDLETB** resources or system with which they come into contact.

No computer user may interfere with or disable the Anti-Virus software installed on their desktop PC. Any virus, virus error messages or security incidents must be reported promptly to ITSupport@ddletb.ie

Do not forward a virus warning to anybody else.

Such warnings are usually hoaxes and are designed to persuade users to delete systems files on their PC; forwarding such a hoax could make **DDLETB** liable for damage to computer systems outside **DDLETB**.

3. E-Mail

Employees have an e-mail account to facilitate the sending and receiving of business messages between staff and between the **DDLETB** and its clients and suppliers. All communications should be done by the organisation e-mail 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.

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

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.

3.1 Risks Associated with E-Mails

- Messages can carry viruses 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.
- 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.

3.2 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**.

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

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 email disclaimer or a link to same must appear at the end of every e-mail sent from your **DDLETB** address to an external address.
- The **DDLETB**'s school/centre 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.
- Corporate e-mail is provided for business purposes.
- Occasional and reasonable personal use of e-mail is permitted provided that this does not interfere with the performance, work duties, responsibilities and customer service of **DDLETB**. It does not support any business other than **DDLETB** and otherwise complies with this policy.
- 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 indecent, obscene, sexist, racist, harassing or other appropriate remarks whether in written form, cartoon form or otherwise is forbidden.
- E-mails must not contain matters which may discriminate on grounds of gender, marital status, family status, age, race, religion, sexual orientation, disability or membership of the Traveller community.
- E-Mails must not contain any inappropriate or lewd content or content likely to cause offence.
- 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 electronic services or other contracts on behalf of **DDLETB** unless you have express Board approval to do so.

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

- If you receive any offensive, unpleasant, discriminatory, harassing or intimidating messages via the e-mail system you must immediately inform your 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 electronic 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.
- When a user registers with a site or a service in the name of **DDLETB** the resulting spamming of information may tie up the communications system. Users must not register with an electronic service over the website without prior permission from their Line Manager and from the ICT Manager, to avoid the release of confidential **DDLETB** information to third parties and to avoid interference with the communications systems.

4. The Internet/Intranet

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

4.1 Rules for Internet use

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

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

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 an employee is downloading pornographic images within view of a colleague or forwarding those images to a colleague, this may result in harassment or sexual harassment by offended parties. Such incidents should 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 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 must not be used to pay for, advertise, participate in or otherwise support unauthorised or illegal activities.
- The Internet must not be used to provide lists or information about the organisation to others and/or to send classified information without prior written approval.

5. Telephone Usage

Access to telephones 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 telephone system.

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.

6. Other Electronic Tools

Other electronic equipment (e.g. photocopiers, cameras, fax machines etc.) remain the property of **DDLETB** and as such must be treated with care and used only for

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019

DDLETB purposes. Abuse of equipment for personal use or gain may result in the use of the disciplinary procedures and in disciplinary action.

7. Plagiarism

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

8. 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.

9. Removable Media

No non-**DDLETB** approved removable media such as CD, DVD, USB drive or SD cards etc. that contain data or files may be used without consulting with the ICT Department.

10. Infringements of Policy

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

- The withdrawal of e-mail and Internet facilities from the Section, Staff or members 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.

11. Encryption

All personal data stored on **DDLETB** mobile 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. This responsibility includes data stored on personal devices.

Policy/ Document No:	PL/016	Version No:	V1.5 November 2017
Previous versions:	N/A	Effective Date:	26/07/2018
Board App/Noting	Jan 2019	Review Date:	24/07/2019