CDETB

An Bord Oideachais agus Oiliúna Chathair Bhaile Átha Cliath
City of Dublin Education and Training Board

CDETB ICT Usage Policy

(Revised April 2018)

Document Number: 0009/2018
Document Type: Policy
Board Meeting: 17th May 2018

Contents

1. Introduction

CDETB's Information and Communication Technology [ICT] resources are provided for the purposes of supporting and enhancing the educational, training, research and administrative services of the Board. Access to ICT resources is provided commensurate with your role. **Once provided, you are the person responsible for ensuring that your use of these resources is in compliance with this policy**. Your line manager or Head of Centre is responsible for verifying that your use of the Board's ICT resources continues to be in line with this policy on an on-going basis. Should you be in **any doubt** as to the appropriate use of any ICT Resource, **ask first**.

Personal use of the Board's ICT Resources is at the discretion of the Board. However, the Board accepts no liability for such use, nor does it guarantee any confidentiality in respect of such use.

CDETB's ICT Resources includes:

- all of the Board's computing and communications equipment
- all electronically accessible data whether the Board's own data or data accessible using the Board's equipment
- all access to internal and external networks including the Internet, websites, chat-rooms and social media
- email accounts using any of the Board's other ICT resources
- software provided or licenced by the Board
- all storage, network, and computing facilities provided by or provided to the Board

These resources remain the property of CDETB. As an employee, student or as someone with whom CDETB has an ongoing relationship, you may be provided with one or more digital identities such as usernames and passwords. These digital identities are provided to you as a means to access certain CDETB ICT resources and should not be disclosed to anyone else at any time. They will be revoked when they are no longer required, usually when a staff member or student ceases to have an ongoing relationship with CDETB. Records, documents or other data associated with a digital identity may be retained by CDETB as defined in the CDETB Records Retention Policy (2018), after a digital identity has been revoked as defined in the CDETB Records Retention Policy (2018).

THIS POLICY APPLIES TO ALL USERS OF THE BOARD's ICT RESOURCES - CDETB STAFF, STUDENTS AND OTHERS WHO ARE FROM TIME TO TIME AUTHORISED TO USE AND/OR ACCESS THE BOARD'S ICT RESOURCES.

2. Material of obscene or offensive nature

Users are subject to the following regulations regarding the use of CDETB's IT/ Communications 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
- 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 Head of IT or HR Manager.

3. Virus protection

Viruses or other threats to the integrity of CDETB's ICT resources can enter an organisation a number of different ways. Some of the more common ways are:

- un-scanned digital storage media (e.g. CDs, DVDs, USB memory sticks) being brought into the organisation
- e-mails or attachments
- downloaded data from the Internet

CDETB's policy is that the use of USBs, SD cards, CDs and other devices is not allowed on the administrative network and will be blocked by electronic means except in exceptional circumstances. Such devices are not blocked on the academic networks in CDETB schools and other centres.

No computer user may interfere with or disable any security software which is installed on any device. Any virus error messages should be reported promptly to it@cdetb.ie

Do not forward a virus warning to anybody else

Some warnings may be hoaxes and are designed to persuade users to take certain actions. This is commonly referred to as Phishing. If you are in any doubt as to the authenticity of any warnings (or indeed messages) that you receive, please first consult with the IT Section before taking any other action.

4. E-mail

Employees have an e-mail account to facilitate the sending and receiving of business messages between staff and between CDETB and its clients and suppliers. All communications should be confined to official channels, including CDETB's corporate email systems.

Every employee has a responsibility to maintain CDETB's image, to use electronic resources in a productive manner and to avoid placing CDETB at any risk. It should be remembered that the contents of e-mail may be considered as official records and may be subject to certain data retention policies and Freedom of Information requests.

4.1 Risks associated with e-mails

- E-Mail attachments may belong to others and there may be copyright implications in sending or receiving them without permission.
- It can be easy to accidently send an email to persons other than the intended recipient (by mistyping the address for example) which might contain confidential or commercially sensitive data. Users should, at all times, take precautions to ensure that any communication originating within CDETB is addressed to the intended recipient
- If you receive an email in error, you should treat it in a professional manner and should not pass it on or share its contents with anyone else.
- E-mails should be regarded as potentially public information which may be subject to Freedom of Information or other legislation.

4.2 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.

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

- CDETB's/school/centre name should be included in the address of all staff members and should be visible to all mail recipients.
- E-mail messages must be appropriate and professional as they reflect the image and reputation of the organisation
- 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 CDETB; it does not support any business other than the CDETB and otherwise complies with this policy
- Distribution lists may only be used in connection with CDETB business.

- Documents prepared internally 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 CDETB unless you have express 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 or the HR manager
- Chain mails or unsuitable information must not be forwarded internally or externally.
- CDETB 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 CDETB'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.
- Users must not register with any electronic service without prior permission from their Line Manager and from the ICT Manager.

5. The internet/intranet

Access to the Internet / Intranet is provided to staff as necessary solely for the purpose of conducting CDETB's business.

5.1 Rules for internet use

- CDETB's Internet connections are intended for activities that either support CDETB's business or the professional development of employees
- Internet usage may be monitored on a systematic basis and as deemed necessary by CDETB
- 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
- It is a disciplinary offence to access, download, save, circulate or transmit any indecent, obscene, child pornographic or adult pornographic material. 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, CDETB 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

5.2 Social Media

CDETB recognises the value of social media which can facilitate communication, learning and collaboration. When using social media 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 social media platforms. Employees should note the use of social media in a work setting is subject to the same guidelines and rules as previously outlined in this policy.

6. Mobile devices

6.1 Mobile phones, tablets, laptops, notebooks, etc. devices provided by the Board

Mobile devices provided to users by the Board must adhere to CDETB's Mobile Phone Policy (2016). Where any device is provided for the purposes of remote access to CDETB resources, CDETB retain full ownership of that device and may take actions to ensure the integrity and security of any data which that device may have access to, including the permanent disabling of that device if there is any concern that it has been compromised

The primary purpose in providing users with these devices is to facilitate the effectiveness of the individual in carrying out his or her duties on behalf of the Board.

6.2 Bring your own device (BYOD) and mobile device management

Users **may not** use their own devices to use or access the Board's administrative or academic network resources. There is one exception, where users may use their own devices to connect to the Board's Wi-Fi or LAN as a guest user. However, no attempt should be made by a user to synchronise a personally owned device with any of the Board's ICT Resources or to logon to the CDETB Domain. User's own devices are not supported by the Board's ICT Support Services and these services must not be engaged for the purpose of supporting these devices for any purpose

7. Software

All software used on the Board's ICT equipment must have a verifiably valid software licence. If you install software of any kind on the Board's ICT Resources, it is your responsibility to ensure compliance with this requirement. No unlicensed software should be installed on any CDETB computers under any circumstances. If you have any doubts about this please contact the IT Section.

8. Acceptable use of or access to the Board's ICT resources

The following is not intended as an exhaustive list, rather it is intended to be indicative of the types of prohibited use or behaviour whilst using or accessing the Board's ICT Resources.

USERS MUST NOT:

- use or access the Board's ICT Resources for any illegal or unethical purpose
- attempt to subvert the integrity of the security of the Board's ICT Resources for any reason
- attempt to subvert any controls or monitoring implemented by the Board's authorised personnel
- use the Board's ICT Resources to use or access other parties' resources or data without the permission of the relevant party
- use or access the Board's ICT Resources for commercial purposes unrelated to the provision of the educational, training, research and administrative services of the Board
- use the Board's ICT Resources to infringe the copyright, patent or other intellectual property rights of any person or organisation
- share IDS, usernames, passwords or other access control features
- process the personal data of others without complying in full with the relevant Data Protection legislation and guidelines in place
- unlawfully copy or retain any of the Board's data or data accessed using the Board's ICT Resources
- engage in behaviour whilst using or accessing the Board's ICT Resources that could bring the Board into disrepute
- use of unlicensed software.
- use of the Board's IT resource to "hack" or break in to an external computer system.

If in doubt about any of the above – please ask!

8.1 Logging, monitoring and control

The Board reserves the right to log and monitor ALL usage of and access to its ICT Resources to ensure technology is being used properly and to use the output from such logging and monitoring to enforce compliance with this policy where appropriate.

The Board also reserves the right to put in place whatever control features it deems appropriate in order to ensure that use of and access to its ICT Resources continues to be for the purposes of supporting and enhancing the educational, training, research and administrative services of the Board.

8.2 Breaches

Should a user become aware of a breach of this policy, this breach should be brought to the attention of the user's line manager or the Head of Centre.

9. Queries

If you have any queries about this policy, please contact the Head of IT.

10. Approval

- This policy was noted by CDETB Board on XXXXX and applies from this date.
- The Board reserves to amend this policy.