
# Dundalk Institute of Technology

# End User Guidelines

# Version 1.1.3

## Document Location

..\DkIT_Policy_Documents\Standards and Guidelines

## Revision History

| Date of this revision: 11/09/18 | Date of next review: |
|---|---|

| Version Number/Revision Number | Revision Date | Summary of Changes | Changes marked |
|---|---|---|---|
| 1.0 | 15/5/15 | Modified by James McCahill | |
| 1.1 | 10/09/15 | Publish Guidelines | |
| v1.1.2 | 11/09/18 | Review document for GDPR | |

## Consultation History

| Version Number/Revision Number | Consultation Date | Names of Parties in Consultation | Summary of Changes |
|---|---|---|---|
| V1.1.2 | 12/09/18 | James McCahill<br>Loretto Gaughran | Review Document wrt GDPR |
| V1.1.3 | 01/11/18 | James McCahill<br>Michael Denihan | Review Document for approval |

## Approval

This document requires the following approvals:

| Name | Title | Date |
|---|---|---|
| James McCahill | IT Manager | 01/11/18 |
| Michael Denihan | Computer Services Manager | 01/11/18 |

End User Guidelines will be reviewed on a periodic basis.

Table of Contents

# 1 Overview

The Institute provides IT services to staff and students (end-users) across each of its Schools and Functions. To safeguard access to these services the Institute must ensures the end user has access these services in a secure and accessible environment.

# 2 Purpose

The purpose of this guideline document is to inform Dundalk Institute of Technology staff, students and external parties on how to act when using Dundalk Institute of Technology IT resources and accessing Dundalk Institute of Technology information assets.

# 3 Definitions

Please refer to Section 2.0 of the IT Documentation Framework for relevant definitions.

# 4 Roles and Responsibilities

| | |
|---|---|
| **IT Manager** | To inform the Vice President for Finance & Corporate Affairs of suspected and/or deliberate non-compliance with end user guidelines. |
| **Staff/Students/External Parties** | To ensure that they follow these end user guidelines when using Dundalk Institute of Technology IT resources and accessing Dundalk Institute of Technology information assets to carry out their job functions or complete their programme of study. |

# 5 Scope

This guideline describes the controls and measures that are necessary to minimise information security risks affecting Dundalk Institute of Technology information assets and IT resources.

It is important to note that All Dundalk Institute of Technology IT resources face information security risks regardless whether access is internal or external, either on Dundalk Institute of Technology equipment or privately-owned devices.

# 6 General End User Guidelines

- Always use Dundalk Institute of Technology IT resources for the purpose for which they were intended.
- In the use of Dundalk Institute of Technology IT resources, always uphold the good name and reputation of Dundalk Institute of Technology.
- Be aware of Dundalk Institute of Technology policies, procedures, standards and guidelines located at https://www.dkit.ie/computer-services/policies-procedures.
- Always report suspected breaches of policies, procedures and standards.

# 7 Portable ICT Devices

Portable ICT devices including phones, laptop computers, "tablets", storage devices, etc., are essential educational / business tools and assets used by Dundalk Institute of Technology on a daily basis. Their portability, however, makes them particularly vulnerable to physical damage, loss or theft.

These devices are especially vulnerable to physical damage, theft or loss including theft of information which may include personal data and implications for GDPR.

Furthermore, as they are often used outside Dundalk Institute of Technology's premises these risks and threats are significantly increased. These devices are more likely to be stolen, and information therein is compromised by people who may not have Dundalk Institute of Technology's interests at heart.

The potential impact of unauthorised access to, usage of, or modification of, important and/or sensitive Dundalk Institute of Technology information can far outweigh the purchase cost of any portable ICT device. The financial costs associated with litigation, risk mitigation and/or reputational loss, because of theft or unauthorised access to information held on Dundalk Institute of Technology portable ICT devices, may be enormous. Consequently, it is essential that custodians / authorised users of Dundalk Institute of Technology portable ICT devices always follow these guidelines.

Many of the guidelines set out in the sections below have a wider application but are referenced here in the context of portable devices.

## 7.1 Physical Security

- The physical security of Dundalk Institute of Technology portable ICT devices, authorised for your use, is your responsibility so you must always take reasonable precautions to secure the device(s). Be sensible and stay alert to the risks.
- Keep all portable devices in your possession and within sight whenever possible, as if it were your wallet, handbag or personal mobile phone. Be extra careful in public places such as airports, railway stations or restaurants, or where large groups of people congregate.
- If you must leave a portable device temporarily unattended in the office, meeting room or hotel room, even for a short while, ensure it is appropriately physically secured/locked.
- Lock the portable device away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a

portable device visibly unattended in a vehicle. If necessary, lock it out of sight but it is generally much safer to take it with you.

- Take reasonable care not to drop or physically damage the portable device.
- Keep a note of the make, model, serial number and the Dundalk Institute of Technology asset label of your portable device but do not keep this information with the device. If it is lost or stolen, notify Dundalk Institute of Technology immediately and inform the IT Help/Service Desk as soon as possible.

## 7.2 Virus Protection

- Viruses are a major threat to Dundalk Institute of Technology portable devices and they are particularly vulnerable if anti-virus and anti-malware software is not kept up-to-date. The anti-virus software MUST be updated at least weekly. The easiest way of doing this is simply to log on to the Dundalk Institute of Technology network for the automatic update process to run. If you cannot log on for some reason, contact the IT Help/Service Desk for advice on obtaining and installing anti-virus updates.
- Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.
- Always virus-scan any files downloaded to your portable device or from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically however the IT Help/Service Desk can tell you how to initiate manual scans if you wish to be certain.
- Report any security incidents (such as virus infections) promptly to the IT Help/Service Desk in order to minimise the damage to the device or to other Dundalk Institute of Technology IT resources.
- Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g.by unusual file activity) by contacting the IT Help/Service Desk. Do not forward any files or upload data onto the network if you suspect your PC might be infected.
- Be especially careful to virus-scan your system before you send any files outside the Dundalk Institute of Technology network. This includes email attachments and CD-ROMs that you create.

## 7.3 Controls against unauthorised access to data on portable devices

- You must use approved encryption software on all Dundalk Institute of Technology portable devices.
    - In windows environment use we use BitLocker to encrypt Laptops Choose a long, strong encryption password/phrase and keep it secure, please refer to the Dundalk Institute of Technology Password standard.
- Contact the IT Helpdesk for further information on device encryption. If your portable device is lost or stolen, encryption provides extremely strong protection against unauthorized access to the data.
- You are personally accountable for all network and systems access under your user ID, so keep your password absolutely secret – read our Password Standard Document. Never share your password with anyone, not even members of your family, friends, colleagues or IT staff.

- IT resources are provided for official use by authorised employees. Do not loan your portable devices or allow it to be used by others such as family and friends.
- Avoid leaving your portable device unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the device.
- Portable devices should be enforced to comply with the following requirements:
    - Must have a password set of at least 4 characters
    - Will automatically lock after 5 minutes if left idle
    - 50 incorrect PIN attempts will result automatic wipe
    - Can be wiped centrally if you report it lost or stolen

## 7.4 Unlicensed software

Most software, unless it is specifically identified as "freeware" or "public domain software", may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and Dundalk Institute of Technology into disrepute by breaking the law.

Do not download, install or use unauthorised software programs. Unauthorized software could introduce serious security vulnerabilities into the Dundalk Institute of Technology networks as well as affecting the working of your laptop. Software packages that permit the computer to be 'remote controlled' (e.g. PCAnywhere) and 'hacking tools' (e.g. network sniffers and password crackers) are explicitly forbidden on Dundalk Institute of Technology equipment unless they have been explicitly pre-authorised by management for legitimate business purposes.

## 7.5 Backups – Portable devices

Unlike desktop PC where the documents folder is backed up automatically by Dundalk Institute of Technology, you must take backups of your own data residing on your portable devices. The simplest way to do this is to logon and upload data from the device to the network drive on a regular basis, ideally daily but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to CD/DVD, USB memory sticks. Make sure that off-line backups are encrypted and physically secured. Remember, if the portable device is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the device.

## 7.6 Laws, regulations and policies

You must comply with relevant laws, regulations and policies applying to the use of computers and information set out by Dundalk Institute of Technology. Software licensing has already been mentioned and privacy laws are another example. Various security policies apply to portable devices, the data they contain, and network access (including use of the Internet).

## 7.7 Inappropriate materials

Refer to Dundalk Institute of Technology Acceptable Usage Policy.

## 7.8 Health and safety aspects of using mobile devices

Mobile devices normally have smaller keyboards, displays and pointing devices that are less comfortable to use than desktop systems, increasing the chance of repetitive strain injury. Limit the amount of time you spend using your mobile device. Wherever possible, place the mobile device on a conventional desk or table and sit comfortably in an appropriate chair to use it. Stop using the mobile device and consult Health and Safety for assistance if you experience symptoms such as wrist pain, eye strain or headaches that you think may be caused by the way you are using the mobile device.

## 7.9 Disclaimer

Dundalk Institute of Technology will not be responsible for any loss of data or applications that resides on your portable device. Dundalk Institute of Technology highly recommends that you backup all the data on your portable device routinely and before trying to connect it to Dundalk Institute of Technology systems. If you forget the PIN for your device, Dundalk Institute of Technology will not be able to retrieve it. The resetting of a new PIN will result in the mobile device being wiped.

./