



Dundalk Institute of Technology

Acceptable Usage Policy

Version 1.0.3

Document Location

..\DkIT_Policy_Documents\Policies

Revision History

Date of this revision: 05/07/18	Date of next review:
--	-----------------------------

Version Number/Revision Number	Revision Date	Summary of Changes	Changes marked
V1.0	20.05.13	Version 1.0 release	
V1.0.1	10/09/15	Annual Review of document noting new official titles	
V1.0.2	18/04/18	Review document for General Data Protection Regulation GDPR go-live	
V1.0.3	05/07/18	Modified Roles and Responsibilities to include SLT	

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
V1.0	09/01/14	James McCahill Peter McGrath Michael Denihan Linda Murphy Loretto Gaughran	Create Policy Document for DkIT
V1.0.1	10/09/15	James McCahill Peter McGrath Michael Denihan	Annual Review - no Changes applied
V1.0.2	04/09/18	James McCahill Loretto Gaughran	Review document for General Data Protection Regulation - GDPR
V1.0.3	24/09/18	James McCahill Michael Denihan	Review Roles & Responsibilities

Approval

This document requires the following approvals:

Name	Title	Date
Governing Body Finance and Risk Committee	M.F. 186.7 Review of IT Policies for GDPR Compliance	12/Mar/2019
Governing Body	Meeting Ref No:G.257.5	7-May-2019

This Policy was noted by the Governing Body on 7-May-2019. It shall be reviewed and, as necessary, amended by the Institute annually. All amendments shall be recorded on the revision history section above.

Table of Contents

1	Overview	5
2	Purpose	5
3	Roles and Responsibilities.....	5
4	Scope.....	6
5	Supporting standards, procedures and Policies.....	6
6	Acceptable Usage Policy	7
7	Monitoring	8
8	Violation of Policy	9
9	Appendices.....	10
9.1	Appendix I – Acceptable Usage Rules for IT Resources and Internet Facilities	10
9.2	Appendix II – Specific Acceptable Usage rules for Email	12
9.3	Appendices III – Specific Acceptable Usage rules for Social Media	13
9.4	Appendices IV – Miscellaneous items.....	15

1 Overview

Dundalk Institute of Technology provides resources to staff, students and external parties to assist them in performing their duties. It is envisaged that these resources will be used for educational, research and administrative purposes.

2 Purpose

The purpose of this policy is to indicate the requirement for responsible and appropriate use of the Dundalk Institute of Technology information technology (IT) resources.

This policy should be read in conjunction with the suite of IT and data protection policies and procedures. The Dundalk Institute of Technology Code of Conduct and Dundalk Institute of Technology Compliance policy are especially relevant for legal and compliance matters. For details on Dundalk Institute of Technology's policy on the management of its social media presence please refer to Dundalk Institute of Technology Social Media Management policy.

3 Roles and Responsibilities

The following roles and responsibilities apply in relation to this Policy:

Governing Body	To review and approve the policy on a periodic basis.
Senior Leadership Team	The Senior Leadership Team is responsible for the internal controls of Dundalk Institute of Technology, The SLT is responsible for: <ul style="list-style-type: none">• Reviewing and approving this Policy and any updates to it as recommended.• Ensuring ongoing compliance with the GDPR in their respective areas of responsibility.• Ensuring oversight of appropriate IT Usage or either through their own work or other governance arrangement.• To ensure the Policy is reviewed and approved by the Governing Body.• To liaise with appropriate staff on information received in relation to potential breaches of the policy.• To ensure the appropriate standards and procedures are in place to support the policy.
IT Manager	<ul style="list-style-type: none">• To define and implement standards and procedures which enforce the policy.

	<ul style="list-style-type: none"> To oversee, in conjunction with data owners, compliance with the policy and supporting standards and procedures. To inform the appropriate SLT members- Vice President for Academic Affairs and Vice President for Financial and Corporate Affairs of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.
Data Protection Officer	<ul style="list-style-type: none"> To monitor and review all aspects of ICT usage to ensure compliance with data protection and privacy obligations. To act as a representative of data subjects in relation to the processing of their personal data. To report directly on data protection risk and compliance to executive management.
Staff/Students/External Parties	<ul style="list-style-type: none"> To adhere to the acceptable usage policy statements in this document. To report suspected breaches of policy to their Head of Department and/or Data Protection Officer.

If you have any queries on the contents of this Policy, please contact the Senior Leadership Team or Data Protection Officer.

4 Scope

This policy applies to:

- Any person who is employed by Dundalk Institute of Technology who receives, handles or processes data during their employment.
- Any student of Dundalk Institute of Technology who receives, handles, or processes data in the course of their studies for administrative, research or any other purpose.
- Third party companies (data processors) that receive, handle, or process data on behalf of Dundalk Institute of Technology.
- The use of IT equipment , software and services (hosted on the DKIT network or in the cloud) which are procured, installed, leased by Dundalk Institute of Technology.

5 Supporting standards, procedures and Policies

- Dundalk Institute of Technology Compliance Policy
- Dundalk Institute of Technology Information Security Policy
- Dundalk Institute of Technology Data Governance Policy
- Dundalk Institute of Technology Social Media Management Policy
- Dundalk Institute of Technology Password Standard.

The above list is not exhaustive and other Dundalk Institute of Technology documents may also be relevant.

6 Acceptable Usage Policy

Conventional norms of behaviour apply to computer-based information technology just as they would apply to more traditional media. Within the setting of Dundalk Institute of Technology this should also be taken to mean that the traditions of academic freedom will always be respected. Dundalk Institute of Technology is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, social class, sexual orientation, age, disability or special need.

Dundalk Institute of Technology encourage all staff, students and external parties to apply a professional attitude towards their individual working environment, including the use of Dundalk Institute of Technology IT resources.

Staff, students and external parties are responsible for their individual user account and password details (Refer to Dundalk Institute of Technology Password Standard).

- Users are forbidden from sharing or using other user's account and/ or passwords. This is in breach of acceptable norms of behaviour and will be dealt with under staff / student disciplinary procedures.
- No staff, student or external party shall jeopardise the integrity, performance or reliability of Dundalk Institute of Technology resources. Reasonable care ¹ must be taken to ensure that the use of resources does not reduce the level of integrity, performance or reliability of Dundalk Institute of Technology IT resources or result in a denial of service to others.
- No staff, student or external party shall improperly/maliciously interfere or attempt to interfere in any way with information belonging to or material prepared by another end user.
- No staff, student or external party shall improperly/maliciously interfere or attempt to make representations on behalf of another end user using that user's username / password.
- Similarly, no staff member, student or external party shall make unauthorised copies of information belonging to Dundalk Institute of Technology, another staff member, student or external party as per GDPR legislation. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.
- Do not redistribute or transmit information intended for internal use to parties who do not require it for Institute business use
- Do not use personal data ² for any purpose other than that for which it was originally obtained.

¹ Staff, Students, and External Parties should reference Dundalk Institute of Technology end user guidelines to ascertain what constitutes reasonable care.

² GDPR regulations 25May2018 <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1490179745294&from=en>

A limited amount of personal usage of Dundalk Institute of Technology resources is acceptable provided it:

- Does not consume more than a trivial amount of resources;
- Does not interfere with department or staff productivity;
- Is not for private commercial gain;
- Dundalk IT resources cannot be used for any activities that are for private personal gain;
- Does not preclude others with genuine Dundalk Institute of Technology related needs from accessing the facilities;
- Does not involve inappropriate behaviour as outlined above, and;
- Does not involve any illegal or unethical activities.

In order to protect the interest of staff, students and Dundalk Institute of Technology system-based controls have been implemented to prevent inappropriate usage³. It is expressly forbidden under this policy to intentionally attempt to circumvent these controls.

While the above policy statements and principles apply to all types of IT resource usage including email, internet and social media, additional policy statements are provided in Appendices I, II and III to further clarify what constitutes appropriate usages of various Dundalk Institute of Technology IT resources.

7 Monitoring

Dundalk Institute of Technology respects the right to privacy of staff, student and external parties. However, this right must be balanced against Dundalk Institute of Technology's legitimate right to protect its interests. Dundalk Institute of Technology is the owner of the IT network, the owner of the IT equipment and services that are provided to staff and students to carry out its legitimate duties.

Dundalk Institute of Technology is committed to ensuring robust information security and to protecting staff, students and external parties from illegal or damaging actions carried out by groups and/or individuals either knowingly or unknowingly. To achieve its aims in this regard, Dundalk Institute of Technology reserves the right to monitor all Dundalk Institute of Technology information resources and Dundalk Institute of Technology data. Any monitoring of Dundalk Institute of Technology data and/or Dundalk Institute of Technology information resources may be random or selective depending on circumstances at that time and will only be conducted following direction from an authorised individual.

All Dundalk Institute of Technology system activity including internet, email and social media activity is monitored and logged for the following reasons:

³ Web Filtering solutions are one example of system based preventive controls.

- Monitoring system performance;
- Monitoring unauthorised access attempts;
- Monitoring the impact of system changes and checking for any unauthorised changes;
- Monitoring adherence to the acceptable usage rules outlined in this policy
- Legal compliance.

When reviewing the results of any monitoring conducted in accordance with this section, Dundalk Institute of Technology will bear in mind that academic members of staff, students and external parties may be in possession of certain material for legitimate teaching, learning and/or research purposes. Academic members of staff, students and/or external parties will not be disadvantaged or subjected to less favourable treatment as a result of Dundalk Institute of Technology monitoring provided they exercise their academic freedom within the law and can demonstrate that their teachings, research or qualifications are relevant to material detected and results revealed by Dundalk Institute of Technology monitoring.

8 Violation of Policy

Contravention of any of the above policy will lead to the removal of Dundalk Institute of Technology resource privileges and can lead to disciplinary action in accordance with the Dundalk Institute of Technology disciplinary procedures. Internet postings which are deemed to constitute a breach of this procedure may be required to be removed; failure to comply with such a request may in itself result in disciplinary action.

9 Appendices

9.1 Appendix I – Acceptable Usage Rules for IT Resources and Internet Facilities

IT resources and internet facilities should only be used for legitimate Dundalk Institute of Technology purposes and comply with the provisions of GDPR legislation.

IT resources and internet facilities should never be used in a way that breaches any of Dundalk Institute of Technology's policies.

In this context, the following policy statements apply:

- Do not bring Dundalk Institute of Technology into disrepute
- Do not breach any obligations relating to confidentiality
- Do not defame or disparage Dundalk Institute of Technology or other staff, students, and/or external parties
- Do not make inappropriate, hurtful or insensitive remarks about another individual or group
- Do not harass or bully another individual or group in any way
- Do not unlawfully discriminate against another individual or group. It is against the law to discriminate against another on grounds of gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of an ethnic minority
- Do not represent yourself as another person
- Do not obtain, store and/or transmit confidential Dundalk Institute of Technology information without appropriate authorisation
- Do not breach data protection legislation (for example, never disclose personal information about another individual online unless this is done in compliance with the relevant GDPR legislation and Dundalk Institute of Technology authorisation)
- Do not breach any other laws or ethical standards
- Respect the legal protections to data and software provided by copyright and license agreements
- Do not load unauthorised and/or unlicensed software onto Dundalk Institute of Technology Resources
- Do not use Dundalk Institute of Technology IT resources to inappropriately obtain, store and/or distribute copyrighted material including music files and movies
- Do not use Dundalk Institute of Technology IT Resources to infringe intellectual property rights including trademark, patent, design and/or moral rights
- Do not obtain/download, store and/or distribute text or images which contain any materials prohibited by law, or material of an inappropriate or offensive nature including pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity
- Do not use Dundalk Institute of Technology computers to make unauthorised entry into any other computer or network
- Do not participate in unauthorised activity which results in heavy network traffic and thereby interrupts the legitimate use by others of Dundalk Institute of Technology resources

- Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse legislation⁴



⁴ Most computer crime related offences can be found in section 5 of the Criminal Damage Act, 1991 and Section 9 of the Criminal Justice (Theft and Fraud) Offences Act, 2001. The Council of Europe Convention on Cybercrime, which entered into force in July 2004, also provides guidelines for governments wishing to develop legislation against cybercrime.

9.2 Appendix II – Specific Acceptable Usage rules for Email

- People should actively seek to use the most appropriate means of communication
- Do not forward inappropriate electronic mail messages to others
- Do not forward email messages where permission has been withheld by the originator
- Do not (without prior notification to IT) forward electronic mail messages with attachments to large internal mail distribution lists
- Do not remove any copyright, trademark or other proprietary rights notices contained in or on the email message
- Do not use email to enter into legally binding contracts without proper authority being obtained beforehand
- Do not use BCC to address recipients inappropriately
- Do not use Dundalk Institute of Technology resources to participant in unsolicited advertising (“spamming”)
- Do not use email resources (@dkit.ie email address) for promoting external /commercial activities

9.3 Appendices III – Specific Acceptable Usage rules for Social Media⁵

The policy statements in this appendix deals with the use of all forms of social media, including but not limited to Facebook, LinkedIn, Twitter, Wikipedia (all other social networking sites and services) and all other internet postings, including blogs, wiki's, and discussion boards.

The policy statements in this appendix applies to the use of social media whether during office hours or otherwise and regardless of whether the social media is accessed using Dundalk Institute of Technology IT facilities and equipment or equipment belonging to members of staff or some other party.

The policy statements below are set out under three headings:

- Protecting Dundalk Institute of Technology's interests and reputation
- Respecting colleagues, students and others
- Protecting Intellectual Property and Confidential Information

Protecting Dundalk Institute of Technology's interests and reputation:

- Dundalk Institute of Technology staff should only use official Institute social media sites for communicating with students and external parties which are managed and moderated as outlined in Social Media Management policy. This includes the use of any social media presence related to the distribution of class materials, study aids, provision of feedback to students or any other supports for teaching and learning activities.
- Staff and external parties must not post disparaging or defamatory statements about:
 - The Institute;
 - It's Staff;
 - It's Students; or
 - Others.
- Staff, Students and external parties should also avoid social media communications that might be misconstrued in a way that could damage Dundalk Institute of Technology's interests and reputation, even indirectly.
- Staff, Students and external parties are personally responsible for what they communicate in social media.
- If your affiliation as a staff member, student or external party of Dundalk Institute of Technology is disclosed, it must be clearly stated that the views presented do not represent those of Dundalk Institute of Technology. For example, you could state, "*the views in this posting do not represent the views of Dundalk Institute of Technology*".

⁵ Staff, Students and/or external parties should refer to Dundalk Institute of Technology Policy for Social Media Management.

- Avoid posting comments about sensitive work-related topics. Even if you make it clear that your views on such topics do not represent those of the Institute, your comments could still damage Dundalk Institute of Technology's reputation.
- Strive for accuracy in any material you post online.
- If you see content in social media that disparages or reflects poorly on Dundalk Institute of Technology or staff, students or external parties of Dundalk Institute of Technology, you should contact your line manager.

Respecting colleagues, students and others:

- Do not post material that could be deemed to be threatening, harassing, illegal, obscene, defamatory, slanderous, or hostile towards any individual or entity.
- Do not post information including personal information related to Dundalk Institute of Technology staff, students and/or external parties without their express permission.
- Do not provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to Dundalk Institute of Technology and create legal liability for both the author of the reference and Dundalk Institute of Technology.

Respecting intellectual property and confidential information:

- Staff, Students and external parties should not jeopardise Dundalk Institute of Technology's business information, confidential information or intellectual property through the use of social media, internet file sharing or internet file storage sites.
- Staff, Students and external parties should avoid misappropriating or infringing the intellectual property of companies and/or individuals, which can create liability for Dundalk Institute of Technology, as well as the individual author.
- Staff, Students and external parties should not use Dundalk Institute of Technology logos, brand names, slogans or trademarks unless approved.
- Staff, Students and external parties should not post any of Dundalk Institute of Technology's confidential or proprietary information without prior written permission.
- Staff, Students and external parties should not post copyrighted material without citing appropriate reference sources or acknowledging copyright accurately.
- Staff should not post information onto external file sharing sites where information may be accessible to external parties without prior permission to do so and having appropriate security measures.

9.4 Appendices IV – Miscellaneous items

Purchase of hardware and Software

All purchases should be approved by the IT Manager, preferably through the IT budget. Use of DkIT purchased hardware only is allowed on the wired network. Do NOT plug a personal laptop into a wall socket – use the wireless network instead. See the separate *Wireless Usage Policy* document.

Installing Software

Get permission from IT Support before you install any software (including public domain software - see Note6) on equipment owned and/or operated by Dundalk Institute of Technology.

Data transfer and storage on the network:

Keep master copies of important data on Dundalk Institute of Technology's network Shares or OneDrive and not on your PC's local C: drive, USB connected storage or private cloud storage. Otherwise it will not be backed up and is therefore at risk.

Ask for advice from IT Support if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring your network to a standstill.

Be considerate about storing personal (non- Dundalk Institute of Technology) files on Dundalk Institute of Technology's network central server environment.

Don't copy files which are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them, or you need to reference them, and the central copies are to be changed or deleted) since this uses up disc space unnecessarily.

Care of equipment

* Don't re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting IT Support.

* Don't take food or drink into rooms which contain specialist equipment like servers. Access to such rooms is limited to authorised Computer Services staff.