Dundalk Institute of Technology

Social Media Management Policy

Version 1.0.4

Document Location

..\DkIT_Policy_Documents\Policies

Revision History

Date of this revision: 6/11/18	Date of next review:

Version Number/Revision Number	Revision Date	Summary of Changes	Changes marked
1.0.0	20/05/13	Version 1.0 release	
1.0.1	10/09/15	Annual Review noting new official titles	
1.0.2	26/03/18	Review document for GDPR go-live on 25-May-2018	
1.0.3	05/07/18	Reviewed Roles & responsibilities section	

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0.0	09/01/14	James McCahill, Peter McGrath, Michael Denihan, Linda Murphy, Loretto Gaughran	Create Policy Document for DkIT
1.0.1	10/09/15	James McCahill Peter McGrath, Michael Denihan	Annual review
1.0.3	10/9/18	James McCahill Loretto Gaughran	Review document for GDPR
1.0.4	6/11/18	James McCahill Michael Denihan	Review document for GDPR compliance

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 should be read in conjunction with Dundalk Institute of Technology Information Security Policy and Dundalk Institute of Technology Acceptable Usage Policy.

This policy was noted by the Governing Body on 7/05/2019. 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

The Institute recognises that communication online and via social networking sites is now an integral part of people's daily lives and affords tremendous possibilities for the promotion of both individual work and of the reputation of the Institute. Members of the Institute community should when possible take advantage of these opportunities to promote themselves and the Institute in a professional manner, however if in doubt about the implications of content you should not publish and seek advice from your Head of Department

2 Purpose

The purpose of this policy is to:

- set direction for the creation, management and moderation of Dundalk Institute of Technology social media presence on appropriate websites including social media platforms,
- refer to the Dundalk Institute of Technology acceptable usage policy for specific acceptable usage rules for social media.
- The scope of this policy also extends to the management and moderation of online communications on internal and external. Dundalk Institute of Technology forums, wiki's, blogs and web technologies yet to become available.

3 Definitions

Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
Records	ISO 15489 defines records as "information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.
Personal Data	Information which relates to a living individual who is identifiable either directly from the data itself or from the data in conjunction with other information held by Dundalk Institute of Technology. Examples of personal data include, but are not limited to: • Name, email, address, home phone number • The contents of an individual student file or HR file • A staff appraisal assessment • Details about lecture attendance or course work marks • Notes of personal supervision, including matters of behaviour and discipline.
Data	As used in this Policy shall mean information which either: - is Processed by means of equipment operating automatically in response to instructions given for that purpose; - is recorded with the intention that it should be Processed by means of such equipment; - is recorded as part of a Relevant Filing System or with the intention that it should form part of a Relevant Filing System;

	- Does not fall within any of the above, but forms part of a Readily Accessible record. Data therefore includes any digital data transferred by computer or automated equipment, and any manual information which is part of a Relevant Filing System.
Data Controller	Means a person or organisation who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, Processed. A Data Controller can be the sole Data Controller or a joint Data Controller with another person or organisation.
Data Processor	Means a person or organisation that holds or Processes Personal Data on the instructions of the Data Controller, but does not exercise responsibility for, or control over the Personal Data. An employee of a Data Controller, or a School or Function within an Institute which is Processing Personal Data for the Institute as a whole, is not a Data Processor. However, someone who is contracted by the Data Controller to provide a service that involves the Processing of Personal Data would be a Data Processor. It is possible for one Institute or person to be both a Data Controller and a Data Processor, in respect of distinct sets of Personal Data. It should be noted however that, if you are uncertain as to whether the Institute is acting as a Data Processor or a Data Controller of Personal Data, it should be treated as being the Data Controller (and therefore comply with this Policy in full) until confirmation to the contrary is provided by the DPO or Legal team.
Third Party	Means an entity, whether or not affiliated with Dundalk Institute of Technology , that is in a business arrangement with Dundalk Institute of Technology by contract, or otherwise, that warrants ongoing risk management. These Third-Party relationships include, but are not limited to, activities that involve outsourced products and services, use of independent consultants, networking and marketing arrangements, merchant payment processing services, services provided by affiliates and subsidiaries, joint ventures and other business arrangements where Dundalk Institute of Technology has an ongoing relationship. Third Party relationships, for the purposes of this Policy, generally do not include student or customer relationships. Under GDPR a 'Third Party' means a natural or legal person, public authority, agency or body, other than the data subject, controller, processor and persons who, under the direct authority of the Data Controller of Data Processor, are authorised to Process Personal Data.
Data Subject	Refers to the individual to whom Personal Data held relates, including: employees, students, customers, suppliers.

Processing	Means any operation or set of operations which is performed on Personal Data or on 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. The terms 'Process' and 'Processed' should be construed accordingly.

4 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: • Reviewing and approving this Policy and any updates to it as recommended by the Data Protection Officer. • Ensuring ongoing compliance with the GDPR in their respective areas of responsibility. • As part of the Institute's Annual Statement of Internal Control, signing a statement which provides assurance that their functional area is in compliance with the GDPR.
Functional / Line Manager	• To monitor compliance with the network security requirements outlined in Section Six of this policy. • To inform their Head of Function and Data Protection Officer of suspected non-compliance and/or suspected breaches of the network security policy (outlined in section six). **Functional / Line Manager** • To define and implement standards and procedures which enforce the policy. • To oversee, in conjunction with Data Owners, compliance with the policy and supporting standards and procedures. • To inform their Head of Function and Data Protection Officer of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.
Data Protection Officer	• To lead the data protection compliance and risk management function, with responsibility for advising how to comply with applicable privacy legislation and regulations, including the GDPR • To advise on all aspects of data protection and privacy obligations. • To monitor and review all aspects of 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	• To adhere to 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.

5 Scope

This Social Media Management policy covers the creation, management and moderation of social media presence on appropriate websites and social media platforms - Refer to the Dundalk Institute of Technology Acceptable Usage policy, Appendix III which outlines acceptable usage rules for social media. The remit of this policy also extends to management and moderation of online communications on forums, wiki's, blogs and new emerging website technologies yet to be developed.

This policy also addresses specific issues around the use of social networking sites and all kinds of online communication, including personal websites and blogs, wikis, discussion boards, email groups and instant messaging. It also covers all kinds of content shared online, including text, photographs, images, video and audio files. The remit of this policy also extends to on-line communication services yet to be developed.

- Any person who is employed by Dundalk Institute of Technology who receives, handles or processes personal data in the course of their employment.
- Any student of Dundalk Institute of Technology who receives, handles, or processes personal data in the course of their studies for administrative, research or any other purpose.
- Third party companies (data processors) that receive, handle, or process personal data on behalf of Dundalk Institute of Technology .

6 Supporting Standards & Procedures

- Dundalk Institute of Technology IT Documentation Framework
- Dundalk Institute of Technology Information Security Policy
- Dundalk Institute of Technology Acceptable Usage Policy
- Dundalk Institute of Technology Compliance Policy
- Dundalk Institute of Technology Data Governance Policy
- Dundalk Institute of Technology Password Standard

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

7 Policy Statements–

7.1 Principles/Creation/Management/Moderation/Online Communications

The Institute recognises the right to dignity of every individual associated with it and it expects that each be treated with consideration, courtesy and respect without harassment or physical or verbal abuse. Every member shall refrain from conduct liable to infringe the rights of others. The Institute's individual codes of conduct requires staff and students to treat others with respect for their person and their rights, whether in the Institute or elsewhere, and to avoid conduct which infringes upon the rights or lawful activities of others, or which brings the Institute into disrepute.

Social networking sites often encourage a level of familiarity, which is at variance with good long-term professional practice. Some social media sites require the user to relinquish any rights to information once posted, so that recalling of previously posted information may be impossible. Although social networking sites might appear anonymous, transactions and messages can be sourced back to the originating computer.

Dundalk Institute of Technology has a public duty to protect its reputation. Where misuse of its logo and other branding products are found, or where it is fraudulently associated with activities or positions, the Institute reserves the right to pursue infringements.

While accepting the right to free speech and expression of ideas, the Institute advises that the following activities can conflict with the Institute's individual codes of conduct. Some of these activities may also be illegal and can be subject to civil or criminal prosecution.

In respect of the use of social networking sites, the Institute's individual codes of conduct may be infringed if staff or students:

- Share confidential information online;
- Post inappropriate comments about colleagues or peers within the Institute or in any professional or social environment;
- Post material which could be construed as bullying, threatening, harassing, illegal, obscene, defamatory, slanderous, or hostile towards any individual or entity.
- Pursue personal relationships with persons in their care, during clinical or work placements;
- Distribute sexually explicit material;
- Trade insults with others online;
- Use social networking sites in any way which is unlawful;
- Provide professional advice unless qualified and authorised to do so;
- Provide personal information on Institute staff or students which infringe on the principles of GDPR.
- Use the Institute brand to imply that you are an employee of the Institute or that you are making representations on behalf of the Institute.

This list is not exhaustive.

7.2 Work-placements, including Internships or Clinical Placements[1]

Students who undertake work placements as part of their studies should note the following:

- Students working with youth groups, community groups, patients or clients should not use social networks to build or pursue relationships with those in their care and with service users, even when the placement terminates. Friendship requests from a current or former patient or person who has been in one's care should be ignored, avoiding the need to give unnecessary offence.
- Work-related matters should never be discussed online, including conversations about those in one's care or complaints about colleagues. Even when anonymised, these are likely to be inappropriate.
- Pictures of those in one's care or of service users should never be published on line, even if those persons request it. Cameras should not be used in the workplace or in the institute without the express permission of staff/students being recorded.
- Social networking sites should not be used for raising and escalating concerns (commonly referred to as whistleblowing). Such matters should be raised with a supervisor or Head of Department.

7.3 Staff

Dundalk Institute of Technology staff must only use official Institute social media sites for communicating with students and external parties which are managed and moderated as outlined here.

- Staff should not use social media channels for distributing class material without permission from Head of Department and individual/group and where appropriate to meet class needs. 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.
- Dundalk Institute of Technology management of social media presence is co-ordinated through a single individual/group appointed by the Dundalk Institute of Technology President.

Dundalk Institute of Technology social media sites must have an official Dundalk Institute of Technology appointed moderator(s) approved by the above individual/group.

The appointed moderator has responsibility on behalf of the Institute for all content published on Dundalk Institute of Technology social media sites for which they have responsibility.

Content must be approved by the moderator[2] prior to publishing.

8 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.

[2] Refer Moderator Guidelines

Dundalk Institute of Technology appointed moderator will monitor content published to Dundalk Institute of Technology social media sites within their responsibility.

9 Policy Compliance

Any on-line activity, which is in breach of the Institute's individual codes of conduct, and/or the code of conduct of a relevant professional body and/or of the Institute's Policy on Bullying and Harassment, including Sexual Harassment will be dealt with under the Institute's relevant disciplinary procedures.

Internet postings which are deemed to constitute a breach of this procedure will be required to be removed by person posting the material or at the request of the institute; failure to comply with such a request will in itself result in disciplinary action where the student or staff member has taken no action to attempt to remove content.

Staff and students have the right to take action if they become the target of complaints or abuse on social networking sites. Most social networking sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others. Those concerned about someone else's behaviour online, should raise their concern with the Head of Department. In the most serious circumstances, for example if someone's use of a social networking site is unlawful, the matter will be reported to the police.

9.1 Guide to Good Practice On-line

- **Personal and professional lives should be kept separate as far as possible.** This applies when using Facebook, Twitter, LinkedIn or any other social networking sites. If you do identify yourself as a staff member or student of Dundalk Institute of Technology make it clear that the views that are expressed are yours and not that of the Institute.
- **Conduct online can have implications beyond one's time as a student.** Inappropriate online behaviour may jeopardise a student's future, in particular, for example in professions where fitness to practice must be established or where on-line behaviour such as hacking may lead to criminal prosecution.
- **Always think twice before posting and consider your audience;** when you are using social media channels, remember that your readers include current/past/future employers, colleagues and lecturers. Consider the aforementioned before you publish and make sure you would be happy for them to read what you have posted.
- **Assume everything posted online is public** and may be assumed to be permanent and likely to be shared, even with the strictest privacy settings. Once something is online, it can be copied and redistributed, and it is easy to lose control of it.
- **Staff and students should protect their own privacy.** Careful consideration should be given to the kinds of information shared with others and privacy settings should be adjusted accordingly.
- **Respect copyrights and fair use** always give people proper credit for their work, and make sure you have the right to use something with attribution before you publish.

9.2 Supporting Documents

- Moderator Guidelines
- Acceptable Usage Policy
- https://www.dkit.ie/system/files/social_networking_policy_09_12_2016_v3.pdf