Dundalk Institute of Technology

Wireless Usage Policy

Version 1.0.3

Document Location

..\DkIT_Policy_Documents\Policies

Revision History

Date of this revision: 06/11/18	Date of next review:

Version Number/Revision Number	Revision Date	Summary of Changes	Changes marked
V1.0.0	20/05/13	Version 0.1 release	
V1.0.1	10/09/15	Annual Document Review	
V1.0.2	25/04/18	Review document for GDPR go-live, Change Roles and Responsibilities section.	
V1.0.3	25/04/18	Review document for GDPR compliance.	

Consultation History

Version Number/Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
V1.0.0	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
V1.0.2	05/09/18	James McCahill Loretto Gaughran	Review Document following GDPR rollout.
V1.0.3	06/11/18	James McCahill Michael Denihan	Review Document following GDPR rollout

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	7-May-2019

This Policy was noted by the Governing Body on 7/05/19 .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 4
2 Purpose 4
3 Definitions 4
4 Roles and Responsibilities 6
5 Scope 7
6 Supporting Standards & Procedures 7
7 Wireless Usage Policy 7
7.1 Agreement 7
7.2 Wi-Fi User Disclaimer 7
7.3 Adding on to the wireless network 8
7.3.1 Procurement 8
7.3.2 School / Function Responsibilities 8
7.3.3 IT Responsibilities 8
8 Monitoring 9
9 Policy Compliance 9

1 Overview

The Institute is responsible for the provision of IT services to users and processing of a significant volume of personal information across each of its Schools and Functions. This is at odds with our need to have a closed secure network system, the Institute provides wireless services to the general user base for general Internet access.

The challenge is to meet both needs adequately, it is important that for Wireless users, that everyone is aware of their responsibilities in relation to data protection as follows:

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 using the wireless infrastructure
- ensure that the configuration of wireless network devices is accurate and does not compromise the security of the wireless/network infrastructure,
- ensure that wireless network is configured accurately and securely and provide a clear statement of the wireless network security disciplines expected to be in place to prevent unauthorised external users from gaining access to information systems and networks and to protect the Dundalk Institute of Technology systems and data from inappropriate access or misuse,
- ensure that only authorised individuals and computing devices gain wireless access to networks and minimise the risk of wireless transmissions being monitored, intercepted or modified,

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 <*Institute Name* >. 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 Subject	Refers to the individual to whom Personal Data held relates, including: employees, students, customers, suppliers.
Systems and Hosts	Means all in-scope hosts (including server, desktop, laptop, network switch, network router/gateway, printer, backup device, etc.)
Encryption	It is the process of encoding information stored on a device and can add a further useful layer of security. It is considered an essential security measure where personal data is stored on a portable device or transmitted over a public network. Refer to the information Security Policies relating to Information Protection for further Guidance on this area
Network Hosts	Means all network host devices directly connected to the Institute's internal network (including network switch, network router/gateway, etc.).
Security Configurations	Are defined security setting checklists (or benchmarks/specifications) that provide detailed low level guidance the appropriate security configuration settings to be applied to each operating systems, middleware systems, database systems and applications. Security configurations settings are also defined for network host operating system configurations.

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, an element of which is the retention of records used in the decision-making process for key decisions in order to demonstrate best practice and the assessment of risk. 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.
IT Manager	• To monitor compliance with the wireless security requirements outlined in Section seven of this policy. • To inform the Vice President for Financial and Corporate Affairs and/or Data Protection Officer of suspected non-compliance and/or suspected breaches of the wireless security policy (outlined in section seven).
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 policy applies to:

- Dundalk Institute of Technology staff
- Dundalk Institute of Technology students
- Dundalk Institute of Technology external parties

6 Supporting Standards & Procedures

- Dundalk Institute of Technology Acceptable Usage 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.

7 Wireless Usage Policy

Dundalk Institute of Technology provides wireless Internet connectivity as a service for staff, students and guests with wireless-enabled devices in open public areas across the campus.

7.1 Agreement

By choosing to use the Dundalk Institute of Technology wireless service, users agree to abide by this Wireless Usage Policy, which prohibits disruptive or illegal activity while using the service.

All end-user devices or systems connecting to the wireless network must comply with the same policies, procedures, and practices governing the use and operation of any end user device or system connecting to the wired network.

All wireless network access shall utilise the Institutes authentication, authorisation and encryption mechanisms prescribed by Computer services.

All authentication and authorisation exchanges at session initiation shall be encrypted.

It is the responsibility of the user to understand these policies and his/her obligation to refrain from inappropriate or illegal activities. Users shall defend, indemnify, and hold the Institute harmless against all claims, actions, and judgments based on or arising out of the users' use of the wireless network or lack of service on said network.

7.2 Wi-Fi User Disclaimer

The user assumes all responsibility for the use of the wireless network.

Dundalk Institute of Technology is not responsible for any alterations of or interference with a laptop's configuration or operation or data files resulting from connection to the wireless network.

Nor is Dundalk Institute of Technology liable for the consequences of wireless network use in any way, including the transmission of computer viruses, loss of data or e-mail, or any harm resulting from the use of an unsecured server.

Dundalk Institute of Technology is not liable for the loss or compromise of any confidential or sensitive, or any other information, and for any and all damages resulting from that loss or compromise. Users should note the Acceptable Usage Policy and user's responsibility for their own data.

In addition, Dundalk Institute of Technology assume no responsibility for damage, theft, or loss of any kind to a user's equipment, software, data files, or other personal property while on DkIT campus or the surrounding area.

It is not guaranteed that all devices will be compatible with the wireless Internet service.

The service is provided "as is" in general public spaces and no support is given to users by any parties.

Users must not share passwords with friends to connect devices to the Wireless network as stated in the acceptable usage policy.

Users must know how to configure and use their own equipment.

Wireless connections may be less secure than a wired connection.

Virus and security protection are the user's responsibility. You must keep anti-virus and operating systems up-to-date.

Finally, this service is not to be used as a permanent connection by anybody. The right is reserved to disconnect and/or ban anyone abusing the service in this or any other manner.

7.3 Adding on to the wireless network

The Institutes wireless network is deployed to service users in public spaces.

If school / functions wish to deploy additional access points into their areas they must note the following to extend the wireless service.

7.3.1 Procurement

School must have budget to procure the wireless Access Points

All wireless access point purchases shall be coordinated through Computer Services.

All wireless access will be operated in such a manner that it will not interfere with other users or the Institutes' wired network/services.

7.3.2 School / Function Responsibilities

Schools / Functions shall request installation, repair, replacement or the move of an existing access point from IT.

Schools / Functions shall be responsible for all costs associated with installation, repair or replacement of access points in its areas of operation.

7.3.3 IT Responsibilities

Computer services is responsible for establishing and maintaining standards for 802.11x wireless access points (equipment and installation) for use at Dundalk Institute of Technology.

All wireless access points shall be installed, configured and managed by Computer Services.

Computer services will maintain a database of access points, their locations, the frequencies in use.

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. 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.

In the case of Wireless devices; all activity is occurring on Dundalk Institute of Technology network systems and all users are subject to the Acceptable Usage Policy, All Dundalk Institute of Technology system activity including internet, email and social media activity is monitored and logged for the following reasons:

- 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 policy
- Legal compliance. - GDPR

9 Policy Compliance

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.