Dundalk Institute of Technology

Information Security Policy

Version 1.0.3

Document Location

.\DkIT_Policy_Documents\Policies

Revision History

Date of this revision: 04/09/18	Date of next review:

Version Number/Revision Number	Revision Date	Summary of Changes
v1.0.0	20/05/13	Version 1.0 release
v1.0.1	30/07/15	Annual Review of document
v1.0.2	04/09/18	Review document for GDPR

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 noting new official titles
v1.0.2	04/09/18	James McCahill, Loretto Gaughran	Review document for GDPR. Changes Roles and Responsibilities
v1.0.3	01/11/18	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	7th-May-2019

This Policy was noted by the Governing Body on 07-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

Dundalk Institute of Technology information systems underpin all of the Institute's activities, and are essential to its teaching, learning, research and administrative functions. Security of information must therefore be an integral part of the Institute's operation and structure to ensure continuity of business, legal compliance and to protect Dundalk Institute of Technology from financial and reputational loss.

The purpose of this policy is to provide a framework to enable the protection of information and information systems from internal and external threats both deliberate and accidental. For the purpose of this policy, information is defined as all records and personal or non-personal data, paper based or electronic, irrespective of the medium or device on which it is stored or of its location.

The Institute is committed to having an effective Information Security Policy Standard in place supported by appropriate procedures, to ensure the confidentiality, Integrity and availability of all information and information systems. Information is an asset which, like other important Institute assets, has value and consequently needs to be protected. Information Security is characterised here as the preservation of:

- Confidentiality – to ensure that information is accessible only to those authorised to have access.
- Integrity – to safeguard the accuracy and completeness of the information by preventing unauthorised interception and manipulation by parties unknown.
- Availability – ensuring that authorised users have access to information and associated assets when required.

The Information Security Policy is a key element of the Information Security Framework. The policy outlines key principles that must be followed when dealing with information to ensure compliance with relevant Data Protection Legislation to which the Institute is subject.

2 Purpose

The purpose of this document is to set out the framework and direction for information security management within Dundalk Institute of Technology. The policy sets out the overall approach to information security and provides a security model aimed at:

- Ensuring the protection of the confidentiality, integrity and availability of all Dundalk Institute of Technology information and information systems, during all stages of information management – input, storage, processing and transmission and reporting. This includes all student, staff, and Institute information;
- Provide a framework to enable compliance with all relevant Data Protection Legislation, regulation and standards;
- Ensure that the Institute has adequate Information Security standards, procedures and controls in place to mitigate Information Security risk;
- Ensure that the Institute has appropriate mechanisms for addressing Information Security incidents
- Clearly outline employee and third-party roles and responsibilities for information security management.

In support of the above objectives, this document:

- Defines the minimum set of actions to be taken by staff throughout the Institute, students and relevant third parties to identify and manage information security risks to which the Institute may be exposed;
- Defines who is accountable for the management of information security risk within the Institute;
- Defines key roles and responsibilities, including those related to the governance of information security risk.

- Dundalk Institute of Technology's Implementing best practices to protect information assets from unauthorized use, disclosure, modification, damage or loss.
- Protecting the work and study environment of staff and students and the good name and reputation of Dundalk Institute of Technology.

Dundalk Institute of Technology information security policy should be read in conjunction with relevant standards, procedures and guidelines which support the implementation of this policy (Refer to section 7).

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.
Sensitive Personal Data	Sensitive Personal Data (or Special Categories of Personal Data) relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life, criminal convictions or the alleged commission of an offence; trade union membership.

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.
Information Security	According to the ISO 27002 standard information security is defined as the preservation of confidentiality, integrity and availability of information
Confidentiality	Confidentiality restricts information access to authorised users.
Integrity	Integrity protects the accuracy and completeness of information through the controlling of information modifications.
Availability	Availability ensures the information is accessible when needed.
Information Asset	The ISO 27002 Standard defines an asset as anything that has a value to an organisation. Information has value and is classified as an asset. Information refers to data that is processed but also encompasses unprocessed data that is stored on Dundalk Institute of Technology's Information Technology (IT) resources.
Information Technology (IT) Resource	All IT systems owned, held under licence or otherwise controlled by Dundalk Institute of Technology including but without limitation to: • Workstations including desktop PCs and laptops; • Servers; • Network technologies such as routers (WAN, LAN and wireless) and associated media and systems; • Printers; • Phones, Smart Phones, tablets and other portable IT devices; • USB and all portable memory devices; • All other media and devices provided by Dundalk Institute of Technology; All other media and devices used to access Dundalk Institute of Technology Information Assets.
Confidential Data	Includes any data covered by GDPR under the category of personal data. This also includes information considered to be commercially sensitive to Dundalk Institute of Technology.
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.
GDPR	Means EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data.
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.
Security Incident	A security incident is made up of one or more unwanted/unexpected or unauthorised security events that could possibly result in a breach to data confidentiality, damage to data integrity or disruption to the availability of data (or service providing access to the data). A security incident may also include a warning that there may be a threat to data or system and host security.

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.
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.
IT 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 the Vice President for Financial and Corporate Affairs and/or Data Protection Officer of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.
HR Office & Registrar's Office	• To follow relevant and agreed disciplinary procedures when HR or Registrar's Office is informed of a potential breach of the Policy. • To manage the disciplinary process.
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.

5 Scope

This Information Security Policy covers security of:

- Dundalk Institute of Technology Information Assets
- Dundalk Institute of Technology IT Resources

This policy applies but is not limited to the following, Dundalk Institute of Technology related groups:

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

Based on the definition of Information Security in section 3, this policy outlines key policy statements relating to these areas.

5.1 Confidentiality

Dundalk Institute of Technology and all staff, students, and external parties of the Dundalk Institute of Technology community are obligated to respect the rights of individuals and to protect confidential data in compliance with the principles of GDPR.

All Dundalk Institute of Technology information is to be treated as confidential unless otherwise indicated. When data is classified as confidential data, appropriate access and security controls are applied in transmission and storage. Confidential data is not to be transmitted without adequate precautions being taken to ensure that only the intended recipient can access the data. Please refer to Dundalk Institute of Technology's Data Governance & Risk management Policy.

Access to information is granted on a need only basis (Refer to Dundalk Institute of Technology User Administration Procedure); Dundalk Institute of Technology staff are granted specific access to allow them to carry out their job functions.

All information is stored in a secure manner; this may require physical and logical restrictions. At a minimum, logical security includes the use of unique identifiers and passwords which are sufficiently complex where staff, students and external parties operate in accordance with Dundalk Institute of Technology password standard.

All hardware used for the storage of Dundalk Institute of Technology data is to be purged of data and securely destroyed once it is no longer to be used. This is to ensure that any data such as licenced software / Intellectual Property / personal information is not released when the IT asset is retired. In this instance hardware can cover a PC / Tablet / Phone that is being retired from use in the institute of technology.

When tapes and other secondary storage devices (CD / DVD Disk / USB device) reach the end of their useful life they are to be purged of Dundalk Institute of Technology Data and securely destroyed.

5.2 Integrity

Access to amend information and/or access to systems which process and record this information is restricted to authorised personnel.

System changes should be completed in accordance with the Dundalk Institute of Technology change management control procedure with which all Dundalk Institute of Technology personnel should be familiar.

An appropriate audit trail including database logs of the creation, amendment and deletion of Dundalk Institute of Technology data and/or systems is maintained by Dundalk Institute of Technology. This is particularly important in relation to the following:

- Data including details on staff, students and suppliers;
- Data including inward fee payments, outward supplier payments, and payroll transactions;
- Dundalk Institute of Technology resource usage data.
- Dundalk Institute of Technology data which may reside outside main Dundalk Institute of Technology system(s).[1]
  Please refer to the Dundalk Institute of Technology Data Governance & Risk Management Policy.

5.3 Availability

To ensure that Dundalk Institute of Technology data and resources are available when required, three key layers of control are employed:

- Prevention of data loss through data back-ups
- Prevention of system downtime and/or unauthorised data access and amendment through anti-virus protection (Refer to Dundalk Institute of Technology Anti-Virus Scanning and Protection Standard)
- Ability to respond to events which prevent data/system access through Disaster Recovery Planning (DRP)

6 Policy

Dundalk Institute of Technology is exposed to several risks arising from the management of Information Security. Failure to manage all or each of the risks identified could result in a detriment to our customers, financial loss to the Council and/or damage to Dundalk Institute of Technology's reputation. These risks include, but are not limited to:

- Deliberate or accidental loss, deletion or corruption of information, for example, leaving documents where the wrong people have access to them

- Theft or accidental unauthorised disclosure of customer or confidential data, for example, emailing sensitive information to the wrong person
- Inaccurate Information/Unauthorised amendments to information, for example, accidental updates to information
- Unavailability of information, for example, information cannot be accessed for business-critical activity.

This policy should not be viewed in isolation. Rather, it should be considered as part of a suite of policies and procedures, the most relevant of which are listed in the Document Information section 7. In particular, Dundalk Institute of Technology's Data Protection Policy should be referenced.

6.1 Policy Requirements for Information Security Risk Assessments

All Schools and Functions must complete an Information Security Risk and Control assessment on an annual basis to identify and document their risks relating to confidentiality, integrity and availability of information.

When Information Security risks are identified, the risk must be assessed, and mitigating controls aligned with the inherent risk must be put in place.

6.2 Policy Requirements for Information Classification and Ownership

All information and Information systems held by the Institute must be classified according to Dundalk Institute of Technology's Information Classification Standards. In broad terms, below is a table listing suggested data classification categories:

Not Classified/Public	Information available to the general public and approved for distribution outside the Institute.
Internal use only	Information not approved for general distribution outside the Institute and which does not clearly fit into the other classifications.
Confidential	Includes data covered by the Data Protection Legislation under the category of personal data (See Note 1 below). Confidential also includes information considered to be commercially sensitive (See Note 2 below) to the Institute, including strategic plans and intellectual property.
Strictly Confidential	Includes data covered by the Data Protection Legislation under the category of sensitive personal data or special categories of personal data (See Note 3 below).

- *Note 1:- Personal Data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information. Examples of personal data include a name, address, contact details etc.*

- *Note 2:- Commercially Sensitive Data relates to any information held by the Institute that if disclosed to an unauthorised party could result in, but is not limited to, the loss of public confidence, non-compliance with regulatory requirements, legal liabilities and additional costs. For example, commercially sensitive information may include, Governing Body reports, senior management board papers, contracts, financial reports, budgets or sensitive project specific information.*

- *Note 3: Sensitive Personal Data (or Special categories of Personal Data) relates to specific categories of personal data which include, amongst other criteria, information relating to the physical and mental health of an individual.*

Methods for managing information must be in line with Information Classification Standards, for example, encryption while emailing Confidential Information outside of the Institute.

All information and information systems must be assigned an owner. Owners are responsible for controlling access to each of their information assets and information systems to a level of security that matches the value those assets.

6.3 Policy Requirements for Internet and Email

Institute internet systems and email systems are provided for Institute business.

Each user is responsible for all activity carried out using these facilities.

6.4 Policy Requirements for Internet and Email Monitoring

The Institute reserves the right to monitor, and given reasonable grounds for investigation to intercept, access and disclose user activities including any email or web-based content such as forms, pictures or documents, created, received, stored or sent by email or over the internet, at any time without notice. The volume, content and recipients of email and web-based content may also be monitored.

6.5 Policy Requirements for Mobile Device Usage

Mobile devices (including laptop computers, mobile phones, smart phones and removable media devices) are the property of the Institute and are provided to Institute employees and authorised third parties for business use. Personally-owned devices cannot be used under any circumstance to store and/or process Institute information.

Each user is responsible for all activities carried out on such a mobile device in the course of their employment with the Institute.

6.6 Policy Requirements for Identity and Access Management

In order to ensure Institute information and systems are adequately protected; the Institute has a robust Identity and Access Management process in place.

All Schools and Functions are responsible for:

- access to information and systems from within the Institute offices or via remote access
- provision of access to information and systems;
- confirmation that access and level of access provided is still required;
- removal of access if/when it is no longer required.

6.7 Policy Requirements for Physical and Environmental Security

The Institute has implemented appropriate controls for physically protecting non-public areas that house information systems.

Each user is responsible to ensure that only authorised personnel, equipment, and media are allowed to and from the Institute's premises. Please also reference Dundalk Institute of Technology's Physical Security Policy for more information.

6.8 Policy Requirements for Personal Data

Personal data is information relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. All Employees, students and relevant third parties must follow these data protection rules when dealing with personal information:

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Retained only for as long as necessary
- Processed in an appropriate manner to maintain security

Personal Data must not be transferred to a country or territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection for the rights of data subjects in relation to the processing of personal data.

6.9 Policy Requirements for Incident/Breach Reporting

Information Security incidents must be reported using the Information Security Incident Management process. Staff and students who have observed or suspect security weakness in or threats to Dundalk Institute of Technology's information systems or services should report to IT, Line Management and the Data Protection Officer (DPO). For incidents, affecting personal data refer to the Data Protection Incident Response & Breach Notification Policy.

6.10 Roles and Responsibilities for Schools and Functions

All Schools and Functions are accountable for effectively managing information security risk within their areas of responsibility, in compliance with the minimum standards stipulated within this Policy Standard.

Schools and Functions must confirm and validate their explicit technical and organisational control requirements for Information Systems which will be implemented and operated by IT. Where a system or an application has been put in place where IT have not been involved, the School or Function holds the IT responsibilities listed below.

6.11 Roles and Responsibilities for IT

In addition to its responsibilities as a Support Function, IT is responsible for:

- Identifying Information Security risks within the shared Enterprise Technology Infrastructure and Systems (e.g. network devices, email systems, file share systems, operating system environments and database environments.)
- Ensuring that the appropriate technical security policies, and standards are developed to protect Information stored, processed or transmitted on Enterprise Technology Infrastructure and Systems and for measuring compliance with these technical security policies and standards.
- Ensuring Enterprise Technology Infrastructure and Systems and their underlying infrastructure components, hosted within IT, have appropriate controls in place to:
    - Prevent and detect a breach in data confidentiality such as security configurations, patching, malware/virus protection, authentication mechanisms, access management, use of privileges accounts and access
    - Prevent and detect damage to data integrity by methods such as system integrity constraints, error handling, data corruption handling, preventing unintentional data changes, audit logging & monitoring.
    - Prevent and detect service disruption through system outages such as system reliance, system fault tolerance, identification and elimination of single points of failure, system failover, system backup and recovery, and system monitoring. IT will support Schools and Functions in confirming and validating their control requirements and will implement and operate same.

6.12 Roles and Responsibilities for DPO

The DPO is accountable for the provision of oversight and challenge of the application of this Policy and independent information security risk oversight and assurance for Dundalk Institute of Technology according to defined criteria including monitoring and independent challenge.

Assisting Schools and Functions by providing advice and guidance on minimum standards, risk management support, and education, awareness and training (including training materials).

Providing reports to relevant governance committees and the SMT in respect of information security risk, including reporting instances of non-compliance.

Assessing the effectiveness of this Policy in meeting its stated objectives.

The Dundalk Institute of Technology Audit & Risk Committee may require the services of Internal Audit to support the DPO in provided independent assurance in the application of aspects of this policy.

7 Supporting Documents

The below is a list of a suite of policies and procedures to be used in conjunction with this policy.

- Data Protection Policy
- Information Security Policy
- Data Governance Policy
- Information Classification and Handling Policy
- Systems Development Life Cycle Policy (Privacy by Design by Default)
- Physical Security Policy
- Clean Desk Policy
- Privileged User Policy
- Data Protection Incident Response & Breach Notification Policy
- Patch Management
- Dundalk Institute of Technology IT Documentation Framework
- Acceptable Usage Policy
- Password Standard
- User Administration Procedure
- Change Control Procedure
- Anti-Virus Scanning and Protection Standard
- Disaster Recovery Plan
-

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

8 Monitoring

Dundalk Institute of Technology reserve the right to monitor all Dundalk Institute of Technology IT resources, information assets, content and data at all times.

Dundalk Institute of Technology reserve the right to log any required Dundalk Institute of Technology data concerning systems access, including data relating to unauthorised access attempts which may warrant investigation.

Dundalk Institute of Technology may also log all changes made to Dundalk Institute of Technology systems and applications.

9 Policy Compliance

9.1 Compliance

Breaches of this policy may result in data breaches under data protection legislation, reputational damage to Dundalk Institute of Technology will lead to the removal of Dundalk Institute of Technology resource privileges and an infringement of the rights of employees or other relevant third parties.

9.2 Compliance Exceptions

Any exception to the policy shall be reported to the Data Protection Officer and IT Manager in advance.

9.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, up to and including dismissal in the case of staff or expulsion in the case of students, being taken in accordance with the Institute's disciplinary procedures. Failure of a third-party contractor (or subcontractors) to comply with this policy may lead to termination of the contract and/or legal action.

Non-compliance shall be reported to the IT Manager and the Data Protection Officer.