Data Handling & Clean Desk Policy

Version 1.0

Document Location

Data Protection Office

Revision History

Date of drafting: April 2019	Date of next review: April 2022

Version Number/Revision Number	Revision Date	Summary of Changes
V 1.0	--	--

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
	11 June 2019	Finance Audit Risk Committee	--

Approval

This document requires the following approvals:

Name	Title	Date
Governing Body		23 Sept 2019

.

This Policy was agreed by the Governing Body on 23 September 2019. It shall be reviewed and, as necessary, amended by the Institute every three years. All amendments shall be recorded on the revision history section above.

Table of Contents

1. Overview

The Institute is responsible for the processing of a significant volume of personal information across each of its Schools and Functions. It is vital that everyone is aware of their responsibilities in relation to data protection as follows:

- It is the responsibility of each School and Function to ensure this personal information is processed in a manner compliant with the relevant data protection legislation and guidance.
- The Institute has an appointed Data Protection Official who is available to Schools and Functions to provide guidance and advice pertaining to this requirement.
- All Staff must appropriately protect and handle information in accordance with the information's classification.
- Personal Data is considered Confidential Information and requires the greatest protection level.

This Policy shall not be interpreted or construed as giving any individual rights greater than those which such person would be entitled to under applicable law and other binding agreements.

2. Purpose

The security and protection of Institute assets, facilities and personnel are fundamental to the efficient and effective operations of the organisation. This policy is to establish the minimum requirements for handling data and maintaining a "Clean desk" - where sensitive/critical information about Institute employees, students, Institute intellectual property, and Institute vendors is handled correctly, is secure in locked areas and out of sight.

3. Roles and Responsibilities

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

Leadership Team	The 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 LT 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. • Ensuring oversight of data protection issues either

	through their own work or a Data Protection Oversight Committee or other governance arrangement.
Finance Audit Risk Committee / Governing Body	To review and approve changes to the policy on a periodic basis upon recommendation from Leadership Team.
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 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 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.

This applies whether you are working in the Institute, travelling or working remotely.

5. Policy

This policy should not be viewed in isolation. Rather, it should be considered as part of the Dundalk Institute of Technology suite of Data Protection policies and procedures (see Appendix A), in particular please refer to Data Handling & Clean Desk Policy for further information on the minimum requirements for handling data and maintaining a "clean desk."

5.1 Policy Requirements

Protecting the integrity of confidential data that resides within Dundalk Institute of Technology is critical. To comply with GDPR regulations, Schools and Functions are encouraged to strive to implement a Data Handling & Clean Desk Policy where appropriate and practicable.

The below requirements must be followed by all staff:

- You should never leave confidential documents unattended at your desk or when working remotely.
- You should never leave confidential documents at printers, in meeting rooms or other such public/semi-public places.
- You should check that no sensitive documents are sitting in your mail slot waiting to be collected and not leave 'Post-it' notes on your desk. These notes often contain personal details such as telephone numbers which ought to remain confidential at all times.
- Information stored in filing cabinets should be reviewed regularly and disposed of in line with the Data Retention Policy.
- If you notice a colleague has left confidential documents unattended, you should put these documents in safekeeping and return to the person concerned as soon as possible.
- Do not bring confidential documentation out of the office unless in accordance with approved business requirements or leave same unattended.
- Always lock your computer screen if away from your desk.
- Always lock away all data carriers, such as files, documents, USB keys, etc. when not required.
- Always secure your paper based files in a locked press.
- Always shred confidential documents or dispose of these in the provided confidential bins.
- Always use a cable lock or locked drawer to secure your IT equipment when leaving it unattended.
- Users shall not leave laptops and other portable computing devices, unattended and in plain sight (for example, in public areas or conference/meeting rooms).
- Users must log off or otherwise lock systems or initiate a password protected screensaver before leaving a workstation unattended (for example, Ctrl+Alt+Del or Windows logo key+L on Microsoft Windows systems).
- While travelling, the Institute’s assets shall not be left in plain sight. Car boots and hotel safes must be utilised to secure assets.

5.2 Data Handling

Dundalk Institute of Technology's documents should be managed in a systematic, structured manner, and information security requirements should be maintained throughout the document lifecycle (i.e., creation, transmission, storage, modification, retention and destruction). The table below publishes the data management requirements for the four data classification levels with the treatment of Confidential and Strictly Confidential data largely the same. Please refer to Data Governance Policy for information on data classification.

	Data Management – EXAMPLE		
Category	Public – EXAMPLE	Restricted/Internal Use – EXAMPLE	Confidential & Strictly Confidential– EXAMPLE
Access Controls	• No restrictions	• Access limited to those with a need to know, at the discretion of the data owner or custodian • Viewing and modification restricted to authorised individuals as needed for Institute-related roles • Authentication and authorisation required for access	• Viewing and modification restricted to authorised individuals as needed for Institute-related roles • Authentication and authorisation required for access • Data Owner required to grant permission for access
Copying/ Printing (both hard and soft copy)	• No restrictions	• Data should only be printed when there is a legitimate business need • Physical copies are prohibited from being left unattended on a printer/fax machine • Physical copies are required to be labeled 'Restricted'	• Data should only be printed when there is a legitimate business need • Physical copies are prohibited from being left unattended on a printer/fax machine • Physical copies are required to be labeled 'Confidential'

Category	Data Management – EXAMPLE		
	Public – EXAMPLE	Restricted/Internal Use – EXAMPLE	Confidential & Strictly Confidential– EXAMPLE
Storage	• Electronic copies are recommended to be stored on a secure server (e.g., publicly posted press release)	• Electronic data is recommended to be stored on a secure server • Encryption of restricted information is at discretion of the owner or custodian of the information	• Electronic data is required to be stored on a secure server • Physical copies are required to be stored in a locked drawer, locked room, or any other area with controlled access • Electronic data is prohibited from being stored on a workstation or mobile device, unless the device is fully encrypted • Storage of regulated confidential data must meet the applicable regulatory requirements • Electronic data is prohibited from being permanently stored on portable media devices (e.g., USB drive)
Transmission	• No restrictions	• Disclosure to parties outside the Institute is required to be authorised by the data owner • Encryption is required when transmitting information through a network (e.g., emails with attachments to third parties)	• Encryption is required during transmission (e.g., SSL, secure file transfer protocols) when transmitting information through a network. Confidential numbers/data may be masked instead of encrypted • Disclosure to parties outside the Institute is required to be authorised by the data owner • Transmission via fax is required to be authorized by the data owner • Transmission of regulated confidential data must meet the applicable regulatory requirements

Category	Data Management – EXAMPLE		
	Public – EXAMPLE	Restricted/Internal Use – EXAMPLE	Confidential & Strictly Confidential– EXAMPLE
Modification	• Modification is restricted to authorised users with a valid business need	• Modification is restricted to authorised users with a valid business need	• Modification is restricted to authorised users with a valid business need • An audit log is required to be maintained in order to track changes made to the data
Destruction	• No restrictions	• Physical copies are required to be shredded • Electronic media containing restricted data is required to be wiped/erased	• Physical copies are required to be shredded • Electronic media containing confidential data is required to be physically destroyed so that data on the media cannot be recovered or reconstructed

6. Policy Compliance

6.1 Compliance

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

6.2 Compliance Exceptions

Any exception to the policy shall be reported to the Data Protection Office in advance.

6.3 Non-Compliance

Failure to comply with this policy may lead to disciplinary action, 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 Data Protection Office.

Appendix A – Supporting Documents

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

- Data Protection Policy
- Data Protection Procedures
- Data Protection Incident Response & Breach Notification Policy
- Data Encryption & Data Anonymisation and Pseudonymisation Policy
- Remote Access Policy
- Physical Access Policy
- Logical Access Policy
- Social Media Management
- Third Party Outsourcing
- Compliance
- Data Governance Policy
- Information Security Policy
- Wireless Security Policy
- Systems Development Life Cycle Policy
- Acceptable Usage Policy
- Privileged User Policy
- Information Security Policy
- Password Standard Procedures
- Anti-Virus Scanning and Protection Standards
- End User Guidelines
- Moderator Guidelines
- Change Control Procedures
- Data Backup and Monitoring Procedures
- User Administration Procedures
- Incident Handling Procedures
- Access to IT Services

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

Appendix B – Glossary of Terms

Content	Content is information with relevant metadata that has a specific use or is used for a particular business purpose.
Records	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.
Metadata	Metadata is a set of data that describes and gives information about other data. It is a description and context of the data. It helps to organize, find and understand data. Examples of metadata include: • Title and description, • Tags and categories, • Who created and when, • Who last modified and when, • Who can access or update.
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.
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.

All other terms used in this Policy and any documents issued in support of this Policy, not referenced in this section, shall have the same meaning as the GDPR and/or local requirements.