Dundalk Institute of Technology

Data Governance Policy

Version 1.0.4

Internal Use Only

Document Location

To be completed by the Data Protection Officer

Revision History

Date of this revision:	**Date of next review:**

Version Number/Revision Number	**Revision Date**	**Summary of Changes**	
V1.0.0		Version 1.0 release	
V1.0.1	10/09/15	Annual review of document noting new official titles.	
V1.0.2	09/02/16	Annual review of document	
V1.0.3	23/03/18	Review document for GDPR go-live on 25-May-2018	

Consultation History

Version Number/Revision Number	**Consultation Date**	**Names of Parties in Consultation**	**Summary of Changes**
Draft v .01	19/04/13	Loretto Gaughran	Initial Review of document
Draft v .02	08/08/13	Loretto Gaughran	Revised / added Data Inventory Items / Forms
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	09/02/16	James McCahill Peter McGrath Michael Denihan	Annual Review
V1.0.3	04/09/18	James McCahill Loretto Gaughran	Review document for General Data Protection Regulation -GDPR go-live on 25-May-2018
V1.0.4	24/09/18	James McCahill Michael Denihan	Review document for approval

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 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

The Institute is responsible for the processing of a significant volume of information across each of its Schools and Functions[1]. 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 information is processed in a manner compliant with the relevant data protection legislation and guidance.
- The Institute has an appointed Data Protection Officer ('DPO') 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.
- Confidential Information requires the greatest protection level (e.g. personal data).

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

To provide direction on the classification, ownership and retention of data and information for Dundalk Institute of Technology as well as clarifying accountability for data and information. Data and information as pertaining to this policy includes electronic and non-electronic data.

Dundalk Institute of Technology is reliant upon the confidentiality, integrity, and availability of its data and information to successfully conduct its operations, meet student and staff/faculty expectations, and provide services.

Therefore, all staff, faculty, students, and external parties of Dundalk Institute of Technology have a responsibility to protect Institute data and information from unauthorised generation, access, modification, disclosure, transmission or destruction and are expected to be familiar with and comply with this policy. Personal data must be managed under the GDPR rules effective 25-May-2018.

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, 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 Office of the Institute Secretary. • 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.
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.
Data Processor	Management and staff within the Dundalk Institute of Technology who take responsibility for processing, storing

	and/or archiving Institute data. Data processors take responsibility to apply the relevant information handling controls required per the classification of data set out in section 5 below.

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

4 Scope

This Data Governance Policy relates to all Dundalk Institute of Technology data including but not limited to:

- Dundalk Institute of Technology Student Data;
- Dundalk Institute of Technology Staff Data;
- Dundalk Institute of Technology Financial Data;
- Dundalk Institute of Technology Commercial Data;
- Dundalk Institute of Technology Intellectual Property
- Dundalk Institute of Technology Academic data

Dundalk Institute of Technology is committed to ensuring that all Dundalk Institute of Technology data is clearly identified, and an inventory of all-important data is drawn up and maintained. The data inventory includes data held on all IT resources and application types. Appendix B provides a template for the maintenance of a data inventory.

This policy applies to:

- Any person who is employed by Dundalk Institute of Technology who receives, handles or processes data in the course of 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.

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 5.1Information Governance

5.1.1 5.1.1Data Ownership

All information and assets associated with information processing facilities (applications) should be owned by a designated part of the organisation. Therefore, data ownership to key sets of information and data (and associated applications) must be formally assigned.

Ownership of data resides with Dundalk Institute of Technology and implies authority as well as responsibility and control. The control of information includes not just the ability to access, create, modify, package, derive benefit from, but also the right to assign these access privileges to others.

In the context of Dundalk Institute of Technology, data ownership responsibility will be formally assigned for the following functional domains/process but is not limited to these functions:

- Secretariat - Governing Body
- President's Office
    - Teaching & Learning
- Vice President for Financial and Corporate Affairs
    - Computer Services IT Manager
    - HR -HR Manager
        - Recruitment
        - Personnel Office
    - Finance Manager
        - Finance Office
        - Payroll processes
- Vice President for Academic Affairs
    - Academic Council
    - Academic Administration & Student Affairs Manager
        - Information Systems
            - Banner
            - Admissions
            - Grants Office
            - Exams

        - Student Services
    - Academic Course Management – Assistant Registrar
    - Research- Research Manager
    - Schools Promotion
        - International Office
        - Erasmus
    - Placement Office
    - Library - Librarian
- Vice President for Strategy, Communications and Development
    - External Services
        - Innovation and Business Development Manager
        - Incubation Centre Manager
    - Estates Manager
    - Marketing & Communications
- School of Business Studies and Humanities
    - Department of Business Studies
    - Department of Management and Financial Studies
    - Department of Humanities
    - Department of Hospitality
    - Lifelong Learning Manager
- School of Engineering
    - Department of Electronic and Mechanical Engineering
    - Department of Civil and Environmental Engineering
    - Department of Building and Surveying
    - Department of Engineering Trades
    - School Research
        - Centre for Renewable Energy at Dundalk IT (CREDIT)
- School of Health and Science
    - Department of Nursing, Midwifery and Health Studies
        - Midwifery Section
    - Department of Applied Science
    - School Research
        - Smooth Muscle Research Centre
        - National Centre for Freshwater Studies (including ORG Research Group)
        - Netwell Centre
        - Electrochemistry Research Group
- School of Informatics and Creative Arts
    - Department of Computing and Mathematics
    - Department of Visual and Human-Centred Computing
    - Department of Music & Creative Media
        - Section of Creative Media
        - Section of Music
    - School Research
        - Creative Media Research Group
        - Centre for Music Research

    - Software Technology Research Centre
    - Individualized Digitized Educational Advisory System
    - Education in Employment, Recognition of Prior Learning
- Resource Planning

Data ownership responsibilities include:

- Approval of user access;
- Approval of user roles/profiles/classes;
- Review of access including application data held in network directory locations;
- Data classification;
- Data retention rules and definition;
- Data transfer and regulation of other parties;
- Master data changes authorisation;
- Ensuring availability of information;
- Data restoration testing;
- Service level management and monitoring.

5.1.2 5.1.2Data Classification

The purpose of information classification is to ensure that information/data receives an appropriate level of data protection.

Following on from this, Dundalk Institute of Technology classifies its data based on the level of impact that would be caused by inappropriate access and/or data loss.

There are three classifications as follows:

Impact Level	**Types of Classification**
High	Confidential data (+ Strictly Confidential Data)
Medium	Internal Use Only data
Low	Public Data

Classification of data is independent of its format.

The following table provides an indication of how classifications get assigned through considering the impact of various risks:

Risk	***IMPACT IS CONSIDERED FROM FOUR MAIN PERSPECTIVES- LEGAL, REPUTATIONAL, FINANCIAL, AND OPERATIONAL***		
Inappropriate access causing breach of confidentiality/data protection rules(GDPR)	Serious	Moderate	Minor
Inappropriate access resulting in unauthorised amendments	Serious	Moderate	Minor
Data loss	Serious	Moderate	Minor
UNAUTHORISED DISCLOSURE	Serious	Moderate	Minor

RESULTING DATA CLASSIFICATION	***Confidential Data*** ***(+ Strictly Confidential Data)***	***Internal Use Only***	***Public Data***
DATA CLASSIFICATION EXAMPLES	• Finance Data relating to students and personnel. • HR Data. • Commercially Sensitive Data • Personal Data (under GDPR Legislation).	• Intranet / Extranet data. • Internal telephone books and directories. • Financial Budgets.	• Public Websites. • Campus Maps. • Staff Directory
	Strictly Confidential • Special Categories of Personal Data (under GDPR Legislation).	•	•

Data that is not yet been classified should be considered **confidential** until the owner assigns the classification.

Confidential Data

Confidential data is information or data protected by statutes, regulations, Dundalk Institute of Technology policies or contractual obligation. Personal data is considered to be **confidential or strictly confidential** data (see distinction above). Prior to the distribution or transmission of confidential data, it is required that reference is made to relevant legislation, (which at this time is the General Data Protection Legislation or GDPR) to ensure such distribution or transmission is not in breach of same. Confidential data should only be disclosed to authorised individuals on a need-to-know basis and in accordance with the relevant legislation. By way of illustration only, some examples of confidential **(C)** and strictly confidential **(SC)** data include:

- CCTV footage;
- Medical records **(SC)**;
- Student records and other non-public student data **(C)** or **(SC)** (see Special Categories of Personal Data under GDPR);
- PPS Numbers **(C)**;
- Personnel and payroll records **(C)**;
- Bank account numbers and other personal financial information **(C)**.
- Financial budgets [Commercially Sensitive – **(C)**].

Confidential data, when stored in an electronic format, must be protected with strong passwords and stored on servers that have appropriate access control measures in order to protect against loss, theft, unauthorised access and unauthorised disclosure.

Confidential data must not be disclosed to parties without explicit management authorisation. Confidential data must only be used for the purpose for which it was originally gathered. If, for legitimate teaching, learning and/or research activities confidential data is used for a purpose other than that of which it was originally gathered the data must be anonymised.

Internal Use Only Data

Internal only data is confidential information that must be protected due to proprietary, ethical, or privacy considerations, and must be protected from unauthorised access, modification, transmission, storage or other use. Internal use data is information that is restricted to members of the Dundalk Institute of Technology community who have a legitimate purpose for accessing such data.

By way of illustration only, some examples of official use data include:

- Intranet / Extranet data.
- Internal telephone books and directories.

Internal Use only data must be protected to prevent loss, theft, unauthorised access and/or unauthorised disclosure.

Public Data

Public data is information that may be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage. Public data can be made available to all members of the Dundalk Institute of Technology community and to all individuals and entities external to the Dundalk Institute of Technology community.

By way of illustration only, some examples of public data include:

- Publicly posted content on all external facing web sites;
- Publicly posted press release;
- Publicly posted schedules of classes;
- Publicly posed interactive Institute maps, newsletters, newspapers and magazines.

5.1.3 5.1.3Retention of Data

It is the responsibility of data owners to clearly indicate the maximum period of time information/data should be retained by the Dundalk Institute of Technology. Refer to Appendix I for the data inventory which should indicate the data retention period. This period of time needs to be agreed in the context of relevant legislation including GDPR guidelines.

Please refer to Data Retention Policy for information on retention periods.

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 or other relevant third parties.

6.2 Compliance Exceptions

Any exception to the policy shall be reported to the Data Protection Officer 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 Officer.

7 Appendix A – Supporting Documents

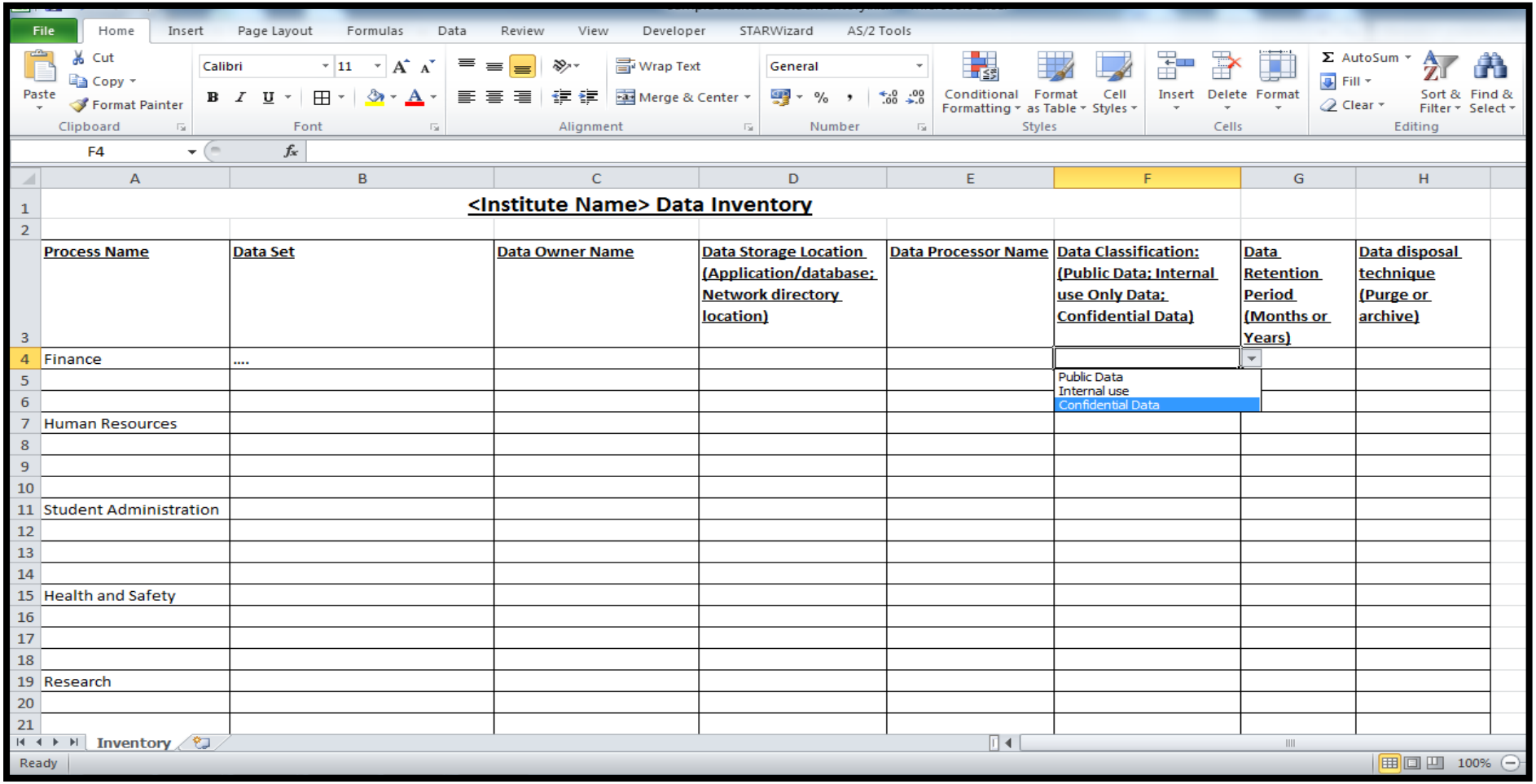
The below is a list of a suite of policies and procedures that may be used in conjunction with this policy this policy.

- Data Protection Policy
- Data Protection Procedures
- Data Retention Policy
- Information Security Policy
-
- Systems Development Life Cycle Policy
- Data Access Management Policy
- Data Handling & Clean Desk Policy
- Data Encryption & Data Anonymisation and Pseudonymisation Policy
- Privileged User Policy
- IT Architecture Security Management Policy
- Data Protection Incident Response & Breach Notification Policy
-

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

8 Appendix B – Data Inventory

Note: Please refer to Data Retention Policy for further information on retention periods.



<Institute Name> Data Inventory

	Process Name	Data Set	Data Owner Name	Data Storage Location (Application/database; Network directory location)	Data Processor Name	Data Classification: (Public Data; Internal use Only Data; Confidential Data)	Data Retention Period (Months or Years)	Data disposal technique (Purge or archive)
4	Finance	....						
5						Public Data		
6						Internal use		
7	Human Resources					Confidential Data		
8								
9								
10								
11	Student Administration							
12								
13								
14								
15	Health and Safety							
16								
17								
18								
19	Research							
20								
21								

9 Appendix C – Guidance on Impact Criteria – Application of Classifications

Note: To be completed by the Vice President for Academic Affairs and Vice President for Financial and Corporate Affairs.

	Minor	Moderate	Serious
Legal	• Failed litigations or litigations which result in payment of no more than €10000. • Minor Compliance breaches.	• Litigations which result in payment of between €10000 and €20000 – • Significant compliance breaches	• Litigations which result in payment of more than €20000. • Serious compliance breach
Reputational	• Adverse internal media attention – Institute publications • Insignificant or no impact on quality framework (including staff, programmes, delivery, research) • Minor Injuries not requiring admission to hospital or minor distress not requiring leave from work/studies to recover	• Adverse local/regional media attention • Injury or distress requiring hospitalisation or leave from work/studies • Significant adverse impact on quality framework (incl. staff, programmes, delivery, research)	• Adverse national media attention and/or adverse social media attention • Serious debilitating injury or loss of life; Serious distress resulting in long term leave • Serious/Pervasive adverse impact on quality framework (Incl staff, programmes, delivery, research)
Financial	• Financial loss equivalent to an annual loss of no more than €100	• Financial loss equivalent to an annual loss of between €100 and €1000	• Financial Loss equivalent to an annual loss of greater than €100
Operational	• Less than two hours downtime in one specific department • Low level of staff /student interruption • Insignificant or no process anomalies	• Half day disruption to several staff and students • Significant irregularity in processes.	• Closure/interruption of entire Institute; or Closure/Interruption of significant portion of Institute for a half day or more • Serious or pervasive irregularity in processes.

RESULTING DATA CLASSIFICATION	***Public Data***	***Internal Use Only***	***Confidential Data***

10 Appendix D – 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 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 Ownership	A process whereby information/data is assigned an appropriate owner whose roles and responsibilities in relation to that information/data are clearly documented. This is also deemed to include any data of an academic nature. Acknowledge nature of Institute – Refer to information security policy on controls over creation, transmission, storage.
Data Classification	A process whereby information/data is classified in accordance with the impact of data being accessed inappropriately, and/or data being lost. The resulting data classification can be associated with a minimum level of control which then needs to be applied when handling data. It is the responsibility of data owners to classify their data.
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.
Confidential Data	Includes any data covered by GDPR under the category of personal data. This also includes information considered to be commercially sensitive to the Institute. Examples include strategic plans or intellectual property.
Strictly Confidential Data	Data covered by GDPR under the category of sensitive personal data or special categories of personal data. If this data were to be disclosed to an unauthorised party, it could result in the loss of public confidence, non-compliance with regulatory compliance, legal liabilities and/or additional costs. Special categories under GDPR include child data and health data.
Data Subject	Refers to the individual to whom Personal Data held relates, including employees, students, customers and students.
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.
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.
Data/Record Retention Schedule	The maximum period of time information/data should be retained by Dundalk Institute of Technology for legal and business purposes. It is the responsibility of data owners to define the retention period for their records/data and the eventual fate of the records/data on completion of this period of time.

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.

11 Appendix E – Guidance on Managing Documentation

11.1 Records Disposition

The Data Inventory Schedule attached to this policy identifies the various types of records held in each area of the Institute. It also identifies how long each record type must be retained before it meets its ultimate fate, e.g., destruction or permanent retention etc. This Disposition overview, as with the Data Inventory Retention Schedule, should be applied in a consistent and regular manner.

It is the responsibility of the relevant appointed person within Schools/Departments/Function – usually an administration staff member at Grade V or VI level depending on functionality – to ensure that records are scheduled as necessary to be retained in the appropriate storage facility or disposed.. In either case, the relevant documentation must be completed e.g., Transfer Form if records are to be removed from office storage space to local dedicated storage space or from dedicated storage to Archive storage. In the case of records, which need to be destroyed, a Records Destruction Certificate should be filled out by the responsible staff member and signed off by the appropriate senior member of staff, usually Head of School/Department or Function.

The way records should be retained will depend on how frequently they need to be consulted.

11.1.1 Current

Records that are consulted on a frequent basis (several times per week) should be retained in the office so they are close to hand. General storage tools should be filing cabinets and/or appropriate shelving with files clearly marked with series data, i.e., title of file, dates, etc.

11.1.2 Non-Current

Records that are consulted on an infrequent basis are classed as non-current and should be stored outside of the office space in a designated store area.

11.1.3 Transfer of Records

Records will need to be transferred from current to non-current status and from non-current to archives or scheduled to be destroyed on a yearly basis, so a record of this transfer process needs to be maintained. See Records Transfer Certificate.

11.1.4 Archives

Records that must be retained permanently must be archived. Records can be deemed to be archive material straight away and archived in not in constant use or maintained in non-current storage for three years and then transferred to Archives (which will be housed in a section of P J Carroll building).

11.1.5 Example of the life cycle of a record

Correspondence records should be kept for a maximum of three years. Current year is current records and should be maintained in office for one year. Then records transferred to non-current status for two years. Thereafter, they should be scheduled for retirement on a yearly basis. Retirement can take the form of destruction, preservation or transfer to archives.

In the case of a record that will need to be kept permanently, the record should be maintained in current record status then transferred to non-current status for two years and thereafter scheduled for transfer to Archive storage.

It is good practice to review records at each stage between current and non-current and between non-current and/or destruction or archiving to assess whether records should be destroyed / archived or retained in non-current storage area for a longer period of time. Some weeding and culling of individual files and series of files may be necessary at this point.

Destruction means the shredding or disposal of both digital and non-digital media. When the retention schedule associated with a file or volume of files has expired, the records administrator should invoke the termination or transfer file/volume process.

11.1.6 Steps to follow in Retirement Phase of Records Management

11.1.7 Step Action Description

1 Review & Preserve

Periodically review the retention schedule of Documents stored documents to find records that are nearing the end of their retention period. Update the retention schedules as required. CD-ROMs or optical discs should also be consulted and after review, a decision is made to remaster the disc to a new medium or to another disc so that records will be preserved for an additional period.

2 Review, transfer

Periodically review the retention schedules of documents stored documents to find records that have reached the end of their retention period. Transfer to an archive those records, which are no longer required for business reasons but may be kept for historical reasons.

3 Review and destroy

Periodically review the retention schedules of documents stored documents to find records that have reached the end of their retention period.

Destroy those records, which are no longer required and have no archival value. It is recommended that hard copy records are shredded on campus. If a large volume of shredding is required external professional services will be used. Soft copy files should be wiped clean.

11.1.8 Termination / Transfer File or Volume Process

- Generate retention and disposal schedules
- Generate transfer schedule
- Cull individual and/or volumes of files
- Delete files and/or volumes
- Prepare and maintain box control lists
- Open new files where necessary and generate new listing for box
- Generate a list of open volumes and files and review for possible closure or disposal
- Generate a list of records for removal to archival records.
- Generate a list of softcopy files to be transferred to dormant storage.
- Generate a list of records scheduled for destruction.
- Get lists signed off by Senior Management staff member.
- Actual disposition of records.

12 Appendix F – Guidance on Managing Standard Forms

<u>Note:</u> To be completed by the FOI Officer<u>.</u>

12.1.1 Records Destruction Certificate

(For Internal Use only)

<table>
<tr><td colspan="5">Retention periods for the below listed records have expired. Please indicate your approval by signing in the approval signatures box. If you disapprove for any reason, mark through the record, initial and state reason for disapproval.</td><td>Date Submitted</td><td>Destruction Cert. No.</td></tr>
<tr><td colspan="5"></td><td></td><td></td></tr>
<tr><td rowspan="2">Record Series Name</td><td colspan="2" rowspan="2">Date Range</td><td colspan="2" rowspan="2">Volume</td><td colspan="2">Approval Signatures</td></tr>
<tr><td>Manager:</td><td>Date:</td></tr>
<tr><td></td><td>From</td><td>To</td><td>Submit</td><td>Dest.</td><td>Sen. Manager:</td><td>Date:</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td colspan="2" rowspan="2">Destruction Certification
I certify that listed records (except those marked as not approved) were destroyed.</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td colspan="2">Job Title:</td></tr>
</table>

					Signature:
					Date Destroyed:
					Method of Destruction: Shredding (in house) Transfer to commercial firm for shredding Other (please specify)

12.1.2 Box Control Listing

School / Department : _____

Department: _____

Box Number: _____

Box Title: _____

Review Date: _____

Destroy /Archive Date: _____

Sequence Range: From: _____ To: _____

Date Range: From: _____ To: _____

12.1.3 Designated Storage Area : _____

DESCRIPTION

This Box List should be attached to appropriate box and copy retained in Office for reference.

12.1.4 Records Transfer Certificate

(For internal use only)

School: _____

Department/: _____

Function

Box Title: _____

Destroy Date:_____

Archive Date:_____

Sequence Range: From: _____ To: _____

Date Range: From: _____ To: _____

D E S C R I P T I O N

Please print:

A copy of this form should accompany the boxed records and a copy kept securely in the School/Function office for reference and record retrieval.