Anonymisation and Pseudonymisation 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.

The General Data Protection Regulation (GDPR) 2018 requires us to use the minimum personal data necessary for a purpose. Secondary uses of personal information must not breach our obligations of confidentiality and respect for private and family life. This guidance identifies how DkIT will use anonymisation and pseudymisation in respecting this confidentiality while still fulfilling our statutory reporting obligations.

Anonymisation and pseudonmymisation enables the Institute to undertake secondary use of personal data in a safe, secure and legal way.

DkIT share and publish information in order to undertake our functions as a Third Level Educational Institute of Technology and we collect personal data through a number of different channels for staff and students. Information collected is likely to incorporate data such as name, address, date of birth, PPS number, staff/student id number and so on. However if identifiable details are removed, information can then be used for secondary purposes such as generating reports to assist us meeting our statutory reporting functionalities without fear of breaching the GDPR.

This process is called anonymization. By removing the personal information elements it allows the Institute work with the required data with fewer restrictions and less fear of breaching data protection safety protocols.

2. Purpose

The purpose of this policy is to ensure a standardised approach to enable consistency throughout the Institute with regard to how and when to anonymise information correctly. This policy should be read in tandem with the full suite of Data Protection and Governance policies.

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
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.
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.
- Third party companies (data processors) that receive, handle, or process personal data on behalf of Dundalk Institute of Technology.
- All must comply with this policy where anonymised information is to be produced or shared from individual level data.

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).

5.1 What is anonymisation and pseudonymisation?

5.1.1 Anonymisation and pseudonymisation both relate to the concealment of an individual's identity.

5.1.2 Anonymisation is the process of removing, replacing and/altering any identifiable information that can point to the person(s) it relates to.

5.1.3 Pseudonymisation is the technical process of replacing the identifying information to protect the individual's identity whilst allowing the recipients to link different pieces of information together. A nickname is an example of pseudonymisation although other identifying information such as age, ethnicity, gender or specific medical conditions may also be changed to prevent identification.

5.2 Definitions

5.2.1 Personal Identifiable Information is any information that can identify an individual. This could be one piece of information or a collection of information for example, a name, address and date of birth.

5.2.2 Primary Use refers to the use of information for the purpose of delivering Institute services to individuals. This also includes relevant supporting administrative processes and audit of the quality of the services provided. Primary use requires information at the person identifiable level.

5.2.3 Secondary / subsequent use is the use of information for a different reason which might be for research purposes. Audits, service management, contract monitoring and reporting requirements. When PII is used in a secondary capacity the information should where appropriate be limited and de-identified so that the secondary use process does not enable individuals to be identified.

5.2.4 Anonymisation is the term for a variety of methods to depersonalise information including statistical production of data so that the specific data subjects cannot be identified. Also included here is aggregation and pseudonymisation.

5.2.5 Aggregation is an anonymisation technique in which information is only presented as totals so that on information pertaining to individuals is shown. The risk here is where there are small numbers in the totals could potentially identify an individual so they may need to be omitted or blurred.

5.2.6 Pseudonymisation is the de-identification of individual information by attaching a code reference or pseudonym to each record that allows the information to be associated with a particular individual without the individual being otherwise identified.

5.2.7 Re-identification or de-anonymisation is where anonymised information is turned back into personal information through the use of for example data matching or combining. Where anonymization is being used the process must be designed to minimise the risk of re-identification.

5.3 Why Anonymise

5.3.1 Anonymisation is undertaken to protect the privacy rights of individuals, while still making data available for statistical or analytical purposes. Personal data is generally used when the intention is to inform individuals of particular decisions relating to them or to provide services to them however where this information is not required it should always be anonymised.

5.3.2 Because personal data relates to living identifiable individuals and that is what GDPR is concerned with, anonymised data does not identify individuals and therefore is not a concern under GDPR as it not recognised as personal data.

6 Compliance

6.1 Breaches

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.

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.

- Data Protection Policy
- Data Protection Procedures
- Data Retention Policy
- Data Governance Policy
- Information Security Policy
- Network Security Policy
- Systems Development Life Cycle Policy
- Data Access Management 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 – 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.