institiúid teicneolaíochta dhún dealgan

DUNDALK
INSTITUTE OF TECHNOLOGY

Employee Confidentiality 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:

Page No:

1. Policy Purpose

Dundalk Institute of Technology employee confidentiality policy is designed to explain how the Institute expects its employees to treat confidential information. Employees will unavoidably receive and handle personal and private information about students, staff, our partners and the Institute. The Institute needs to ensure that this sensitive information is well-protected.

We must protect information because:

- We have a legal obligation to protect personal information given to us in confidence (e.g. student and staff details) for a designated purpose.
- Failure to properly secure and protect confidential business information can lead to the loss of business contacts and will affect the image of the Institute.
- In the wrong hands, confidential information can be misused to commit illegal activity (e.g., fraud or discrimination), which can in turn result in costly litigation.
- The disclosure of sensitive employee and management information can lead to a loss of employee trust, confidence and loyalty.

2. Scope

This policy is for all employees of Dundalk Institute of Technology. It is also for Governing Body members, students/researchers, contractors, or volunteers who may have access to confidential information.

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. Policy Elements

What Type Of Information Must Be Protected?

Confidential workplace information in DkIT can generally be broken down into three categories: employee / student information, management information, and business information.

Employee / Student Information: We have an obligation under data protection legislation to collect, maintain and use personal data only for the purpose for which it is originally collected and we must have the explicit consent of individuals to do so. For example, a name on its own is not necessarily personal data, however add to that a date of birth, address, PPS number, student number for example and that is then classed personal, add to that a photography and its classed as more sensitive personal information as the person is more readily identifiable.

Management Information:

Confidential management information can includes discussions about employee relations issues, disciplinary actions, terminations, workplace investigations of employee misconduct, etc. While disclosure of this information isn’t necessarily “illegal,” it is almost always counterproductive and can seriously damage the collective workings of the Institute.

Business Information:

Confidential business can refer to information that's not generally known to the public and would not ordinarily be available outside of the Institute until such time as it released officially unless via illegal or improper means. Common examples of confidential business information might include, business plans, financial data, budgets and forecasts, computer programs and data compilation, client or student lists, research data, membership lists, supplier lists, etc. Business information does not include information that we would voluntarily give to potential students or staff, post on our website, or otherwise freely provides to others outside of the Institute.

Confidential information examples are:

- Personal data of staff and students
- Data of partners / suppliers
- Patents, formulas or new technologies
- Data given to us in trust by any of our partners
- Document and processes explicitly marked as confidential
- Unpublished goals, forecasts, initiatives marked as confidential
- Unpublished financial information

Employees may have various levels of authorized access to confidential information.

5. Employee Guide:

As an employee you should:

- Lock or secure confidential information at all times.
- Shred confidential documents when they are no longer required in line with Institute practice
- Make sure you only view confidential information on secure devices
- Only disclose information to other employees when it is necessary and authorized
- Confidential documents must be kept on the Institute campus unless it is absolutely necessary to move them.

As an employee you should not:

- Use confidential information for any personal benefit
- Disclose confidential information to anyone within the Institute unless authorized to do so
- Disclose confidential information to anyone outside of the Institute.
- Replicate / copy confidential documents or files and store them on insecure devices.

When an employee terminates employment with the Institute, or moves departments within the Institute, they are obliged to return any confidential files and delete any files held on their personal devices relating to their most recent post.

6. Precautionary Measures:

The Institute will take precautionary measures to safeguard confidential information by

- Storing and locking paper documents
- Encrypting and password protecting electronic information and data bases
- Maintaining a security access log
- Adopt a risk management approach to the collation and maintenance including destruction of confidential information.

7. Exceptions:

- Confidential information may sometimes have to be disclosed for legitimate reasons. Examples are:
- Revenue – we are legally obliged to share payroll data with Revenue Commissioners for application of relevant taxes to employees.
- Other disclosures might be discretionary – should a request for information come in from An Garda Siochana as part of an ongoing investigation the privacy impact would have to be considered.

8. Disciplinary Consequences

Employees who do not adhere to the employee confidentiality policy will face disciplinary and possibly legal action. Any breach of this policy will be thoroughly investigated and any willful intentional breach of confidentiality guidelines will be treated extremely seriously. Unintentional breaches of this policy depending on frequency and seriousness may also face disciplinary action.

Appendix A.:

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.