Dundalk Institute of Technology

Privileged User Policy

Version 1.0.2

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
1.0.1	31/08/18	Added GDPR content -Initial Review

Consultation History

Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0.1	31/08/18	James McCahill Loretto Gaughran	Moved Definitions Section to chapter 3
1.0.2	31/08/18	James McCahill Michael Denihan	Review for GDPR compliance

Approval

This document requires the following approvals:

Name	Title	Date
James McCahill	IT Manager	6/11/18
Michael Denihan	Computer services Manager	6/11/18

This Policy 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 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 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.
- 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 purpose of this policy is to ensure that processes and tools and in place and used to track, control, prevent, correct the use of, assignment, and configuration of administrative privileges on computers, networks, and applications.

3 Definitions

Privileged User	A privileged user is a user who, by virtue of function, and/or seniority, has been allocated powers within the computer system, which are significantly greater than those available to the majority of users.
Administrative privileges	Having administrator privileges (sometimes called admin rights) means a user has privileges to perform most, if not all, functions within a system, computer, operating system, or database. For example, these privileges can include such tasks as installing software and hardware drivers, changing system settings, installing system updates. They can also create user accounts and change their passwords. Note: A single computer can have more than one administrative account.

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 Glossary of Terms section, shall have the same meaning as the GDPR and/or local requirements.

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.

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. • 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 Senior Leadership Team or Data Protection Officer.

5 Scope

This policy applies to all Institute employees (permanent and temporary), students, vendors, independent contractors, consultants and other persons or entities that use Dundalk Institute of Technology IT resources, during and outside of working hours.

6 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 and IT policies and procedures (see Appendix A).

6.1 Policy Requirements

The below requirements must be adhered to in order to ensure that the access of all privileged users is managed correctly:

- Ensure that end-user account with administrative privileges and administrative accounts are only used when explicitly required.

- Ensure that Administrators only have access to end-user accounts with administrative privileges or administrative accounts with a documented and legitimate business justification.

- Ensure that an inventory of all administrative accounts and all accounts with administrative privileges is maintained and validated at regular intervals to ensure that each person with access to administrative privileges is authorised with a current and legitimate business justification. Evidence of each user validation review and justification for access must be maintained.

- Ensure that administrators are required to access all system and hosts using a fully logged and non-administrative end-user account and transition to an administrative privilege account when required to carry our administrative tasks or duties requiring elevated access.

- Ensure that third party administrators are required to use a dedicated and hardened connection gateway server and/or dedicated machine for all administrative connections to the in-scope systems, hosts and network devices in order to perform administrative tasks or tasks requiring elevated access.

- Ensure sensitive privileged user activity is subject to audit logging and monitoring as outlined in the Dundalk Institute of Technology Audit Logging and Monitoring Management policy.

7 Policy Compliance

7.1 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.

7.2 Compliance Exceptions

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

7.3 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.

8 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
- Systems Development Life Cycle Policy
- Data Encryption & Data Anonymisation and Pseudonymisation 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.