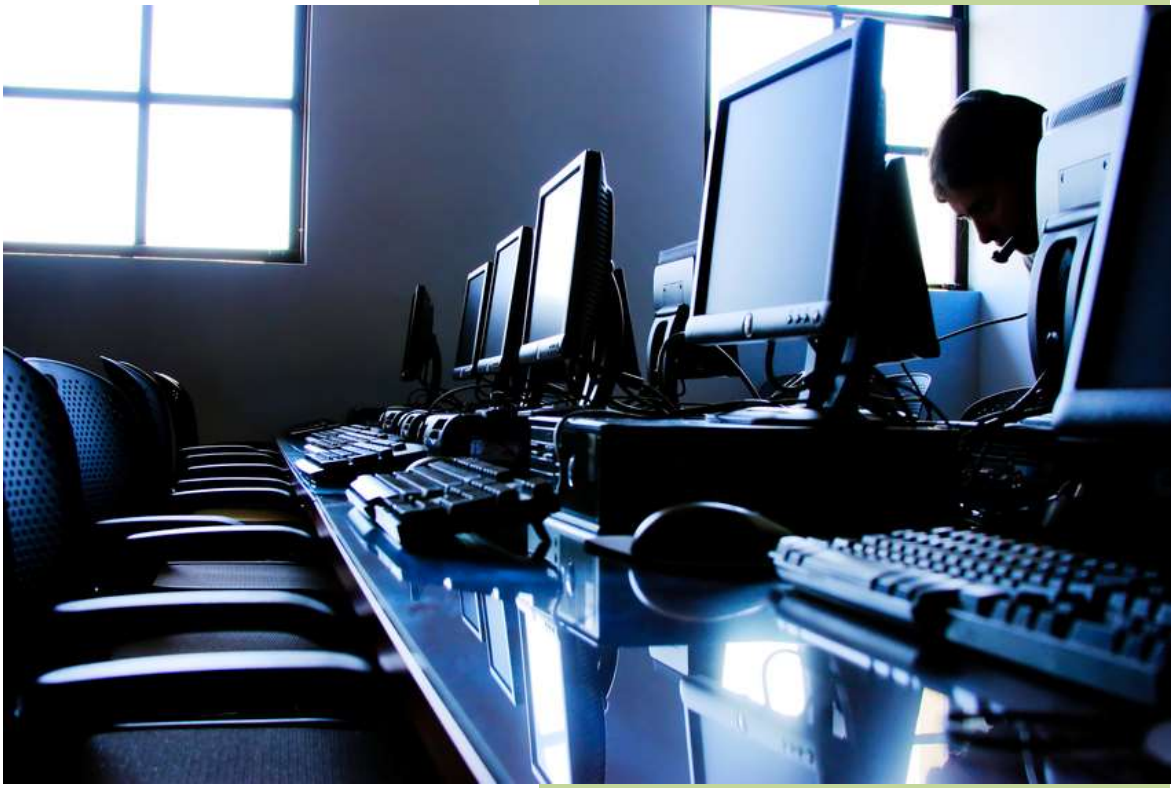
IADT Data Roles and Responsibilities Policy

Document Reference and Version No	ICT DATA/RRP Version 1
Purpose	The purpose of this policy is to facilitate and formalize the roles and responsibility requirements related to the stewardship of IADT's data
Commencement Date	August 2017
Date of Next Review	August 2020
Who needs to know about this document	All Staff
Revision History	First Version
Policy Author	ICT Manager
Policy Owner	Sec/Fin Controller

IADT Data Roles and Responsibilities Policy



Information Services Division

Dun Laoghaire Institute of Art Design and Technology

1.0 TABLE OF CONTENTS

1.0 PURPOSE

The purpose and objective of this policy is to facilitate and formalize the roles and responsibility requirements related to the stewardship of IADT's data. This standard specifically supports the Data Classification Policies each faculty/department and functional should hold.

2.0 SCOPE

Support all IADT's policies plus any National and EU regulations governing the protection of the Institute's data.

3.0 DEFINITIONS AND ABBREVIATIONS

3.1 Definitions

Data Owners – Individuals employed by IADT who have been given the responsibility for the integrity, accurate reporting, and use of physical and computerized data.

3.2 Abbreviations

EU: European Union

IADT: Dun Laoghaire Institute of Art, Design and Technology

ICT: Information and Communication Technology

ISD: Information Services Division

Sec/Fin: Secretary/Financial Controller

4.0 RESPONSIBILITY

Executive: Sectary/Financial Controller
Central Management: ICT Manager

5.0 PROCEDURE

The objective of this policy is to facilitate and formalize the roles and responsibility requirements related to the stewardship of IADT's data. This standard specifically supports the Data Classification Policies each faculty/department and functional hold, but also exists to support all other IADT policies plus any National and EU regulations governing the protection of the Institute's data.

5.1 Data Owner

The individual assigned by management to oversee the proper handling of administrative, academic or research data. The owner is responsible for ensuring that appropriate steps are taken to protect data and for the implementation of policies, guidelines and memorandums of understanding that define the appropriate use of the data. The development by the data owner of a formal data classification and access policy would highly recommended.

The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments. The owner or his designated representatives are responsible for and authorized to:

- Approve access (electronic and/or physical) and formally assign custody of an information resources asset.
- Specify appropriate controls both electronic and physical (were appropriate), based on data classification, to protect the information resources from unauthorized modification, deletion/destruction, or disclosure. The owner will convey those requirements to administrators for implementation and educate users. Controls shall extend to information resources outsourced by IADT (e.g., An Cheim and Glenbay Storage).
- Confirm that applicable controls are in place to ensure appropriate level of confidentiality, integrity and availability.
- Confirm compliance with applicable controls.
- Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures.
- Ensure access rights are re-evaluated when a user's access requirements to the data change (e.g., job assignment change).

5.2 Data Administrator or Data Controller

IADT or outsourced service provider charged with implementing the controls specified by the owner. The administrator is responsible for the processing, storage and recovery of information. The administrator of information resources must:

- Implement the controls specified by the owner(s).
- Provide physical and procedural safeguards for the information resources.

- Assist owners in evaluating the overall effectiveness of controls and monitoring.
- Implement the monitoring techniques and procedures for detecting, reporting, and investigating incidents.

5.3 Data User

The user is any person who has been authorized by the owner of the information to read, enter, or update that information. The user has the responsibility to:

- use the resource only for the purpose specified by the owner.
- comply with controls established by the owner.
- prevent disclosure of confidential or sensitive information.

The user is the single most effective control for providing adequate security.

5.4 Data Classifications

Information classification is to ensure that information/data receives an appropriate level of protection and security. Following on from this, IADT 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:

1. Public data
2. Protected data
3. Confidential data

Classification of data is independent of its format.

The data classifications exist to aide in understanding what data types can be released and what security controls should exist to protect each data type. 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 (REFER TO APPENDIX II FOR FURTHER GUIDANCE)		
Inappropriate access causing breach of confidentiality/data protection rules	Minor	Moderate	Serious
Inappropriate access resulting in unauthorised amendments	Minor	Moderate	Serious
Data loss	Minor	Moderate	Serious
UNAUTHORISED DISCLOSURE	Minor	Moderate	Serious
	↓	↓	↓
RESULTING DATA CLASSIFICATION	***Public Data***	***Protected Data***	***Confidential Data***
	↓	↓	↓
DATA CLASSIFICATION EXAMPLES	Public Websites. Campus Maps. Staff Directory.	Intranet / Extranet data. Internal telephone books and directories. Financial Budgets.	Finance Data. HR Data. Human Subject Data

If you have questions regarding the classification of specific data, and the following definitions cannot answer them, always consult the data owner(s).

5.4.1 Confidential Data

IADT data that cannot be released and is protected by:

- IADT, National or EU law or regulations (e.g., contacts of employment).
- Contractual agreements requiring confidentiality (e.g., Non Disclosure Agreements).
- Declared confidential by the appropriate person in IADT
- Specific data to be protected as specified by the Data Protection legislation.

Protect your confidential data by applying the appropriate security guidelines. Please contact the data owner(s) if you have any questions regarding how to secure confidential data.

Data that is not yet been classified should be considered confidential until the owner assigns the classification. Long term classification of Data as confidential for this reason is not acceptable.

5.4.2 Protected Data

IADT data that is not otherwise identified as "Confidential Data" or Public data which must be appropriately protected to ensure a lawful or controlled release (e.g. Freedom of Information Act requests). It can also be known as Internal Use Only data.

Unless your data is known to be confidential or public, consider it Protected. Please contact the data owner(s) if you have any questions regarding how to secure or release protected data.

5.4.3 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. Data is public if:

- There is an obligation to make the data public (e.g. Annual Reports).
- The information is intended to promote or market the IADT, research or institutional initiatives (e.g., www.iadt.ie content)

Data Owners should restrict access to data that:

- Are not intended for a specific use by a specific person or audience
- Could be used to exploit an individual, system or institution

6.0 Further Information

If you have queries in relation to this policy, please contact:

ICT Manager

Dun Laoghaire Institute of Art Design and Technology

Tel: 012394777

Email: ict_manager@iadt.ie