# Encryption Policy

**Version 1.0**

This policy may be updated at anytime and without notice to ensure changes to DkIT's organisation structure and/or business practices are properly reflected in the policy. Please ensure you check the DkIT webpage for the most up to date version of this policy.

## 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. Purpose

The purpose of this policy is to define the acceptable use and management of encryption software and hardware throughout the Institute (DkIT).

This policy is mandatory and by accessing any Information Technology resources which are owned or leased by the Institute, users are agreeing to abide by the terms of this policy.

## 2. Scope

This policy takes precedence over all other relevant policies which are developed at a local level and applies to:

- All information technology (IT) resources provided by DkIT;
- All users including Institute staff, students, contractors, sub-contractors, agency staff and authorised third party commercial service providers of the Institute's IT resources;
- All connections to (locally or remotely) the Institute network domains;
- All connections made to external networks through the Institute network.

## 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:<br>• Reviewing and approving this Policy and any updates to it as recommended by the Data Protection Officer.<br>• Ensuring ongoing compliance with the GDPR in their respective areas of responsibility.<br>• 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.<br>• 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<br>• To advise on all aspects of data protection and privacy |

| | |
|---|---|
| | obligations.<br>• To monitor and review all aspects of compliance with data protection and privacy obligations.<br>• To act as a representative of data subjects in relation to the processing of their personal data.<br>To report directly on data protection risk and compliance to executive management. |
| **Staff/Students/External Parties** | • To adhere to policy statements in this document.<br>• 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

### 4.1 Principles of Encryption

Where possible all confidential and restricted information must be stored on a secure DkIT network server with restricted access. Where it has been deemed necessary by a Manager (at APO level, equivalent or above) to store confidential or restricted information on any device other than a DkIT network server the information must be encrypted.

All confidential and restricted information transmitted by email to an email address outside of the Dundalk Institute of Technology domain (ie one that does not end in @dkit.ie) must be encrypted.

All passwords used as part of the process to encrypt/decrypt information must meet the standards requirements in the DkIT Password Policy. Please refer to the following link to access information on Password Standards, Anti-Virus Scanning and Protection Standard and End User Guidelines. These documents should be read in tandem with this policy.
**https://www.dkit.ie/computer-services/policies-procedures/standards-guidelines**

### 4.2 Servers

Confidential and restricted information stored on shared DkIT network servers must be protected by the use of strict access controls and encryption software.

### 4.3 Desktop Computers

- DkIT desktop PCs are generally accepted as having a lower risk of being stolen and as such most will not need to have encryption software installed however the following types will require it:

- Desktop computers which for business, geographic or technical reasons need to permanently store DkIT confidential or restricted information locally on the computer's hard drive. (as opposed to the DkIT secured network).

- Desktop computers which for business, geographic or technical reasons need to permanently host DkIT information systems (eg MS Access, Excel etc) that process DkIT confidential or restricted information locally on the computer's hard drive. (as opposed to the DkIT secured network).

- Desktop computers used by DkIT staff to work from home.

- Desktop computers which are located in unrestricted areas which are open to the public (eg Reception desks etc).

- Desktop computers which are located in third party facilities.

The preferred method of encryption for DkIT desktop computer devices is whole disk encryption.

**4.4 Laptop, Mobile Computer and Smart Devices**

- All laptop computer devices must have DkIT approved encryption software installed prior to their use within Dundalk Institute of Technology. In addition to encryption software the laptop must be password protected and have up to date anti-virus software installed.
- You must also use approved encryption software on other DkIT portable devices.
- The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Devices which are not capable of whole disk encryption must use file/folder level encryption to encrypt all confidential/restricted information stored on the device.
- You must choose a strong encryption password/phrase and keep it securely. You should refer to the Institute's Password Standard document and contact the IT Help Desk for further information on device encryption. If your portable device is lost or stolen, encryption provides extremely strong protection against unauthorised access to the data.
- You are personally accountable for all network and systems access under your user ID so do not share your password with anyone, not even family members, friends or colleagues.

- Portable / mobile devices are provided and authorised to staff for official use only. Do not loan your devices or allow access to it by others such as family or friends.
- These devices must not be used for the long term storage of confidential and restricted information.

### 4.5 Removable Storage Devices

- All confidential and restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, they must be stored in a locked cabinet or drawer when not in use.
- Removable storage devices except those used for backup purposes must not be used for the long term storage of confidential and restricted information.
- The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt all confidential and restricted information stored on the removable storage device.

### 4.6 USB Memory Sticks

- Confidential and restricted information should not be stored on memory sticks.
- In exceptional circumstances where it is essential to store or temporarily transfer confidential or restricted information an encrypted memory stick approved by Dundalk Institute of Technology IT Services may be used. The storage of such data on any other USB memory stick will be considered a breach of this policy.
- Memory sticks must not be used for the long term storage of confidential or restricted information. This information must be stored on a secure DkIT network server.
- Confidential and restricted information stored on the DkIT approved memory stick must not be transferred to any internal (except a secure DkIT network server) or external system in an unencrypted form.

### 4.7 Transmission Security

- All confidential or restricted information transmitted through email to an email address outside of the DkIT domain (i.e. one that does not end in @dkit.ie) must be encrypted.

## 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.