Letterkenny Institute of Technology

Guideline for Storing Electronic Research Data

Version 1.1

Document Location

This document will be stored on the LYIT website. Master and hard copy will be held by the IT Manager.

Revision History

Date of this revision: 01/10/2018	**Date of next review:** 01/10/2019

Revision Number	Revision Date	Summary of Changes	Changes marked
1	01/12/2013	First Version	
1.1	3/12/2018	Addition to include GDPR	

Approval

This document requires the following approvals:

Title	Date
IT Manager	October 18
Vice President for Academic Affairs and Registrar	October 18

This Guideline for researchers will be reviewed on a periodic basis.

Table of Contents

1. PURPOSE

The purpose of this guideline document is to provide specific guidance to researchers and students at Letterkenny Institute of Technology (LYIT) in relation to protecting research data stored or data transmitted electronically. This guideline should be read in conjunction with Letterkenny Institute of Technology's Information Security Policy and Encryption Protection Standard.

2. DEFINITIONS

Encryption: is the conversion of data into a form called cipher text that cannot be easily understood by unauthorised people. The purpose of encryption is to protect confidential or personal information during transmission over the network or unauthorised access in the event a portable device or removable media is lost or stolen.

Removal Media: refers to storage media which is designed to be removed from workstations easily. Examples of removable media commonly include: USB flash drives, external hard drives, optical disks (DVDs, CDs, and Blu-Ray discs), floppy disks, magnetic tape, portable music, cameras or smartphone device.

Portable Devices: refers to laptops, netbooks, tablets, mobile smartphones and E-book readers.

Personal Data: according to the Data Protection Acts 1988-2018, personal data is data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in or is likely to come into the possession of a data controller.

Confidential Data: is data that should not be available or accessible to the public. Such data may include financial, commercial, research, and Intellectual property data. The unauthorised or accidental disclosure of this data could seriously and adversely impact LYIT.

2. SCOPE

This document outlines the general guidelines to be followed by LYIT students and researchers to protect research data. Security practices must be factored when storing research data in electronic format on any computer hardware device. Most of the data collected for research can be classified as data that is not generally available to the public. Data on human subjects maybe governed by Data Protection Act 2018 (www.dataprotection.ie) requiring appropriate security measures taken to protect against unauthorised access, or unauthorised disclosure.

Following the steps outlined in section 2.1 – 2.4 will greatly improve security of your data reducing the risk of unauthorised access, or unauthorised alteration, disclosure or destruction of the data.

2.1 GENERAL GUIDELINES

General Guidelines:

- Do not store or copy confidential data to unencrypted hardware. This includes USB memory sticks, removable hard drives, and optical media such as CD or DVD ROM.
- Do not store data on college computer equipment within general usage areas (e.g. Library, Computer Labs) or computer equipment that you do not personal own or manage.
- Never share passwords with other people who are not approved to work on your research.
- Use encryption software to encrypt confidential or personal data.

2.2 PERSONAL COMPUTER SECURITY

Personal Computer Security refers either to your home Personal Computer (PC) or Laptop (Portable Device).

1. Set Password for access to the computer.

Your computer must be configured so that when it starts up, you need to enter a password. This should be a strong password that is only used by you.

2. Regularly update your software.

Without up-to-date software, your computer connected to the Internet can be extremely vulnerability to hackers, viruses, spyware and malware. The most important step to securing your personal computer is making sure you have all the current updates to the operating system (Microsoft Windows 10/8/7, Apple Mac or LINUX) and software packages installed.

3. Anti-Virus Software.

Anti-virus software will protect your computer free of malicious software such as viruses, worms, Trojans, Spyware, Malware and Adware.

It's recommended to purchase commercial anti-virus software such as Norton Antivirus, McAfee or free anti-virus such as AVG. Note: recommend to compare anti-virus products, various anti-virus software products can offer different levels of protection.

All antivirus should be set for daily automatic updating.

4. Ensure Firewall running.

In addition to antivirus software, firewall should be running on your computer. A firewall monitors network traffic into and out of your computer system and attempts to block connections that appears hostile. It is recommended to use the Firewall built into the Microsoft Windows operating system.

5. Password-Protected Screen Saver

Unless your computer is in a secure, private space accessible only by you, recommend to implement password-protected screen savers that activate after no more than fifteen minutes of inactivity.

6. Document Passwords

Sensitive Word, Excel and PowerPoint files should be password protected

2.3 CONFIDENTIAL DATA

If your computer holds confidential data, particularly personal data that is govern by Data Protection Act 2018, your computer must be kept in a secure location, or it must be physical locked down or the confidential data must be encrypted, and password protected.

Encryption of confidential data on computers and particularly portable devices (laptops, USB memory stick) is strongly recommended.

There is a variety of encryption software for common operating systems. Some software encrypts the entire hard disk, while other has an option to encrypt specific files or folders on the hard disk. Some operating system, such as Microsoft Windows have options to turn on the operating systems built-in encryption software. There are also some readily available data encryption products from third party vendors. Some are even free.

If you encrypt Institute data, you should not be the only person who knows the password needed to unlock it. Your supervisor should have some process to securely store a copy of the password, so that data can be retrieved in any eventually.

Please refer to LYIT's Encryption Protection Standard for further information on encryption technology and guidelines.

It is important to note that encryption technology wrongly used can result in data loss.

2.4 BACKUP DATA

The local data owner is responsible for the backup of data that does not reside on Institute servers. Data owners should implement backup of research data on daily\weekly basis as appropriate to their needs. Your backup data should be kept in a secure location, or it must be physical locked away.