Institute of Technology, Sligo

End User Guidelines

Version 0.2

Document Location

The document is held on the Institute's Staff Portal here.

Revision History

Date of this revision: 28/03/16	Date of next review:

Version Number/Revision Number	Revision Date	Summary of Changes	Changes marked
0.1	25/11/14		
0.2	28.03.16	Replaced Head of Development and Business Operations with Secretary/Financial Controller or nominated member of the Executive Committee	

Approval

This document requires the following approvals:

Name	Title	Date
	Executive Committee	26.09.17

End User Guidelines will be reviewed on a periodic basis.

Table of Contents

1. PURPOSE

The purpose of this guideline document is to inform IT Sligo staff, students and external parties on how to act when using IT Sligo IT resources and accessing IT Sligo information assets.

2. DEFINITIONS

Please refer to Section 2.0 of the IT Documentation Framework for relevant definitions.

3. ROLES AND RESPONSIBILITIES

Staff/Students/External Parties

- To ensure that they follow these end user guidelines when using IT Sligo IT resources and accessing IT Sligo information assets to carry out their job functions or complete their programme of study.

IT Manager

- To inform the Secretary & Financial Controller or nominated member of the Executive Committee of suspected and/or deliberate non-compliance with the end user guidelines.

4. SCOPE

This guideline describes the controls and measures that are necessary to minimise information security risks affecting IT Sligo information assets and IT resources.

All IT Sligo IT resources face information security risks.

5. GENERAL END USER GUIDELINES

- Always use IT Sligo IT resources for the purpose for which they were intended.
- In the use of IT Sligo IT resources, always uphold the good name and reputation of IT Sligo.
- Be aware of IT Sligo policies, procedures, standards and guidelines.
- Always report suspected breaches of policies, procedures and standards.

6. MOBILE ICT DEVICES

Mobile ICT devices including mobile phones, smart phones, laptop computers, tablet devices, storage devices, etc., are essential educational / business tools and assets used by IT Sligo on a daily basis. Their portability, however, makes them particularly vulnerable to physical damage, loss or theft.

Furthermore, as they are often used outside IT Sligo's premises, these risks and threats are significantly increased and theft by people who do not work for IT Sligo, or may not have its interests at heart, are significant risks that need to be effectively managed.

Mobile devices are especially vulnerable to physical damage, theft or loss, or theft of information, including personal data stored on these devices.

The potential impact of unauthorised access to, usage of, or modification of, important and/or sensitive IT Sligo information can far outweigh the purchase cost of any mobile ICT device. The financial costs associated with litigation, risk mitigation and/or reputational loss, as a consequence of theft or unauthorised access to information held on IT Sligo mobile ICT devices, may be enormous. Consequently, it is essential that custodians / authorised users of IT Sligo mobile ICT devices follow these guidelines at all times.

6.1 Physical Security

- The physical security of IT Sligo mobile ICT devices, authorised for your use, is your responsibility so you must take reasonable precautions at all times to secure the device(s). Be sensible and stay alert to the risks.
- Keep all mobile devices in your possession and within sight whenever possible, as if it were your wallet, handbag or personal mobile phone. Be extra careful in public places such as airports, railway stations or restaurants, or where large groups of people congregate.
- If you have to leave a mobile device temporarily unattended in the office, meeting room or hotel room, even for a short while, ensure it is appropriately physically secured and/or locked.
- Lock the mobile device away out of sight when you are not using it, preferably in a strong cupboard, filing cabinet or safe. This applies at home, in the office or in a hotel. Never leave a mobile device visibly unattended in a vehicle. If absolutely necessary, lock it out of sight but it is generally much safer to take it with you.
- Take reasonable care not to drop or physically damage the mobile device.
- Keep a note of the make, model, serial number and the IT Sligo asset label of your mobile device but do not keep this information with the device. If it is lost or stolen, notify IT Sligo immediately and inform IT Services as soon as possible.

6.2 Virus Protection

- Viruses are a major threat to IT Sligo mobile devices and they are particularly vulnerable if anti-virus and anti-malware software is not kept up-to-date. The anti-virus software MUST be updated at least weekly. The easiest way of doing this is simply to log on to the IT Sligo network for the automatic update process to run. If you cannot log on for some reason, contact the IT Services for advice on obtaining and installing anti-virus updates.
- Email attachments are now the number one source of computer viruses. Avoid opening any email attachment unless you were expecting to receive it from that person.
- Always virus-scan any files downloaded to your mobile device or from any source (CD/DVD, USB hard disks and memory sticks, network files, email attachments or files from the Internet). Virus scans normally happen automatically however the IT Services can tell you how to initiate manual scans if required.
- Report any security incidents (such as virus infections) promptly to IT Services in order to minimise the damage to the device or to other IT Sligo IT resources.
- Respond immediately to any virus warning message on your computer, or if you suspect a virus (e.g. by unusual file activity) by contacting IT Services. Do not forward any files or upload data onto the network if you suspect your PC might be infected.
- Be especially careful to virus-scan your system before you send any files outside the IT Sligo network. This includes email attachments and CD-ROMs that you create.

6.3 Controls against unauthorised access to data on mobile devices

- You must use approved encryption software on all IT Sligo mobile devices, choose a long, strong encryption password/passphrase and keep it secure, please refer to the IT Sligo Password Policy for more information. Contact IT Services for further information on device encryption. If your mobile 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 keep your password absolutely secret. Never share it with anyone, not even members of your family, friends or Institute staff.
- IT resources are provided for official use by authorised employees. Do not loan your mobile devices or allow it to be used by others such as family and friends.
- Avoid leaving your mobile device unattended and logged-on. Always shut down, log off or activate a password-protected screensaver before walking away from the device.
- Mobile devices will be enforced to comply with the following requirements:
    - Must have a password set of at least 6 characters
    - Will automatically lock after 5 minutes if left idle
    - 50 incorrect PIN attempts will result automatic wipe
    - Can be wiped centrally if you report it lost or stolen

6.4 Unlicensed software

Most software, unless it is specifically identified as “freeware” or “public domain software”, may only be installed and/or used if the appropriate licence fee has been paid. Shareware or trial packages must be deleted or licensed by the end of the permitted free trial period. Some software is limited to free use by private individuals whereas commercial use requires a license payment. Individuals and companies are being prosecuted for infringing software copyright: do not risk bringing yourself and IT Sligo into disrepute by breaking the law.

6.5 Backups – Mobile devices

Unlike IT Sligo’s network resources, which are backed up automatically by IT Sligo, you must take your own backups of data on your mobile devices. The simplest way to do this is to logon and upload data from the device to the network on a regular basis, ideally daily but weekly at least. If you are unable to access the network, it is your responsibility to take regular off-line backups to CD/DVD, USB memory sticks. Make sure that off-line backups are encrypted and physically secured. Remember, if the mobile device is stolen, lost or damaged, or if it simply malfunctions, it may be impossible to retrieve any of the data from the device.

6.6 Laws, regulations and policies

You must comply with relevant laws, regulations and policies applying to the use of computers and information set out by IT Sligo Software licensing has already been mentioned and privacy laws are another example.

6.7 Inappropriate materials

Refer to IT Sligo’s Acceptable Usage Policy.

6.8 Disclaimer

IT Sligo will not be responsible for any loss of data or applications that resides on your mobile device. IT Sligo highly recommends that you backup all the data on your mobile device routinely and before trying to connect it to IT Sligo systems. In the event that you forget your PIN, IT Sligo will not be able to retrieve it. The resetting of a new PIN will result in the mobile device been wiped.