Acceptable Usage Policy

12 September 2023

Version 1.1

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

Document Details	
Document Title:	Acceptable Usage Policy
Version:	1.1
Approved By:	Governing Body
Date Approved:	12 September 2023
Effective Date:	12 September 2023
Next Review Date:	6 September 2026
Policy Owner:	Vice President Corporate Affairs

Revision History			
Previous Version No.	**Summary of Amendments**	**Approval date**	**Version No.**
n/a	Approved by Governing Body	26 July 2022	1.0
1.0	**6 September 2023 - reviewed by the Policy Review Group:** Recommended to extend for 3 years and submit to the Governing Body for approval	_	1.1
1.1	Approved by Governing Body	12 September 2023	1.1

Consultation Details		
Name:		
Date:		
Details of Consultation:		

Publication Details	
Where	**Date**
SETU Website	Version 1.1 (12 September 2023)
Drive/Public/HR/Policies	
All Staff Email	

Feedback or issues arising on implementation of this policy should be communicated to the policy author.	
Policy Author	Computing Services Managers

Table of Contents

1. Purpose

The purpose of this policy is to indicate the requirement for responsible and appropriate use of the South East Technological University's (SETU) Information Technology (IT) resources.

SETU is committed to providing its users with the widest possible range of computing resources, including e-mail, internet access, networking and information resources, to support its mission of teaching, research, and community engagement. The provision of an efficient and reliable computing and networking service depends on the cooperation of all users. It is therefore important that all users are aware of their responsibilities to other users and to the providers of services.

All Users must utilise the resources in a responsible manner and must respect the integrity of computer systems, networks and data to which they have access, and follow any rules and regulations governing their use. The purpose of this policy is to safeguard individual users and to ensure the integrity and reliability of the computer system. This is not intended to limit an individual's use of SETU's computer resources; rather it is designed to ensure that SETU can offer the widest possible service to its users.

2. Scope

This policy covers acceptable usage of all SETU's Information Technology (IT) resources, including data.

This policy applies to all users (which may include, but is not limited to, staff, students, researchers, employees, retired employees, contractors and any third parties) operating on behalf of the University or a subsidiary of the University).

3. 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	• To ensure the Policy is reviewed and approved by the Governing Body. • To consult as appropriate with other members of the Executive and Management Teams. • To liaise with the Registrar's Office or Human Resources (HR) on information received in relation to potential breaches of the policy. • To ensure the appropriate standards and procedures are in place to support the policy.

IT Managers	• To define and implement standards and procedures which enforce the policy. • To oversee, in conjunction with data owners, compliance with the policy and supporting standards and procedures. • To inform the VPs for Academic Affairs & Registry / VPs for Corporate Services & Finance of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.
Staff / Students / Researchers /Employees /Retired Employees / Interns / Contractors / Third Parties operating on behalf of the University or subsidiary of the University	• To adhere to policy statements in this document. • To report suspected breaches of policy to their Head of Department or the IT Manager.
HR Office	• To follow relevant and agreed disciplinary procedures when informed of a potential non-compliance • To manage the disciplinary process

If you have any queries on the contents of this Policy, please contact the IT Managers or the Senior Leadership Team.

4. Policy

The computer resources of the university may not be used for illegal acts or for activities in breach of SETU policies. Likewise, SETU resources may not be used for personal/commercial activity unless specifically authorised by VP for Corporate Services or designated appointee. Minor incidental personal usage of the university's computer resources is permitted but should be limited. Only staff of SETU, registered students or other approved users may use SETU's computer resources. Unauthorised use may lead to disciplinary action or prosecution under appropriate legislation.

It is the policy of SETU to maintain the highest standards of security for its IT resources and to minimise risks to the confidentiality, integrity and availability of those resources, in the interests of all users.

The drafting of this policy has been influenced by the legislation included in Appendix A.

4.1. Security

The university has implemented various security safeguards and controls, including network protection, identity management, firewalls and desktop protection, to achieve maximum security and uptime of its IT systems.

4.1.1. Personal Accounts

Users will be provided with personal accounts and passwords to permit access to the university's network and other computer resources. Users must take reasonable precautions to prevent unauthorised use of such accounts. In addition, staff must ensure, in so far as is reasonably practicable, that the computers in their office or under their control are not used for unauthorised purposes. Advice and practical help are available from the Computing Services Departments to help safeguard data, systems and computer equipment.

4.1.2. Viruses & Malicious items

Users must take reasonable care to ensure that they do not transmit viruses or other malicious computer code to other users. Refer to the SETU's *Anti-Virus standard* for guidelines on protecting your computers.

4.2. Regulatory Compliance

4.2.1. Software Licenses

Users are not permitted to install any software unless it is appropriately licensed. Where SETU site licenses permit off-campus use and/or personal use, users must adhere to the terms and conditions of such licenses.

4.2.2. Electronic Data Integrity

Electronic data are recognised under the same law as paper-based documentation and is subject to the same requirements in terms of protecting the integrity, accessibility, accuracy and confidentiality of such data. If you keep personal data on others, you must comply with the provisions of the General Data Protection Regulations (2016) as described in SETU's *Data Protection* policy. You should also be aware that the Freedom of Information Act (1997) applies to records held in electronic format.

4.3. Best Practice standards

4.3.1. Use of IT facilities

Staff and students must behave reasonably in their use of SETU's computer resources. They must not undertake or facilitate any activity that could jeopardise in any way, the integrity, reliability and performance of these resources.

Wilful damage (or attempted damage) to computer resources may result in disciplinary action or prosecution under appropriate legislation. Likewise, deliberate wasteful use of resources and time (e.g. downloading vast amounts of unnecessary data, printing large amounts of superfluous information) could lead to withdrawal of services and/or disciplinary action.

It is not acceptable to view, download, transmit or store any obscene or indecent images or material (unless there is a legitimate academic reason for doing so). Nor is it acceptable to attempt to access any files, data or records which the individual has not been authorised to access. SETU's computer systems may not be used to publish or transmit anything that is libellous, unfounded, or defamatory or is damaging to another computer system. Such action may be regarded as a serious disciplinary matter.

4.3.2. Processing & Storing Data

SETU data should only be stored on SETU's network or cloud storage (Network drives, Onedrive, Teams folders, Sharepoint or Dropbox). Access to the SETU's network storage is restricted to legitimate users and files are protected and backed up as part of the Computing Services Department's backup schedule. Confidential information must not be stored locally on an employee's desktop or laptop computer.

Data should not be downloaded or exported from Application Systems or Databases without prior approval of the data owner. Users that have received unnecessary or excessive privileges to confidential data should contact the data owner to have those privileges revoked.

Members of staff should use the Computing Services Department's authorised remote access facilities (e.g. VDI, VPNs, Windows Virtual Desktop) when processing confidential data offsite. These facilities provide secure access to SETU's central resources and negate the need to use portable devices and portable media. If it is not possible to use the SETU's authorised remote access facilities, confidential data must be stored in encrypted form when processing data offsite.

Using a personal account to store confidential data, with externally hosted storage providers, is not permitted. This includes personal or free accounts with providers such as Dropbox, GoogleDrive, Onedrive, iCloud, etc. Refer to the SETU's *Cloud Storage Policy* for further information on using externally hosted storage providers.

4.3.3. Use of Portable Devices

Using portable devices and personal computers when processing confidential data poses a high risk. These devices are vulnerable to loss, theft, corruption, viruses, cyber-attacks, etc.

Avoid using portable devices, portable media or personal computers when processing confidential data, unless there is no other viable alternative. If there is a business-driven requirement to use these devices, confidential data must be encrypted (Refer to *SETU*'s *Encryption Policy* for details regarding encryption). Computing Services Staff can advise on how to implement this level of security.

Portable devices and personal computers that are used for processing confidential data should be stored securely when not in use and should not be left unattended in cars, on trains, etc. (Refer to *SETU's Portable Device Guidelines* for recommendations on using portable devices). Any loss or theft of these devices should be reported immediately to your line manager and to the IT Manager.

4.3.4. E-Mail

The primary purpose of the SETU's e-mail system is to promote effective communication for the teaching, learning, research and operational activities of the university. Please refer to *SETU's Email Policy* for further information on appropriate usage of email.

4.4. Privacy and Monitoring of Information

All information residing on university systems is the sole property of SETU, subject to the university's *Intellectual Property* policy. SETU respects the privacy of users. It does not routinely inspect, monitor or disclose electronic messages. However, the IT Manager or designated nominee may access any individual's account, without the user's consent, if required by law or where there are reasonable grounds to believe that violation of the law or SETU policy may have taken place or where failure to do so may hamper the SETU's operations.

Users should be aware that, during the performance of their duties, certain members of Computer Services staff, who operate and support the electronic communication facilities (e-mail and internet access) may need to monitor transmissions or observe certain transactional information to ensure the proper functioning of the systems. On these and other occasions they may inadvertently observe the contents of electronic communications. Except as provided by law or this policy, they are not permitted to hear, see or read the contents of electronic communications intentionally, observe transactional information that is not germane to the foregoing purpose, or otherwise disclose what they have heard, seen or read.

In the event that Computer Services personnel discover violations of law or policy in the course of their duties they shall report all such occurrences to the IT Manager.

5. Violation of Policy

Contravention of any of the above policy could lead to the removal of SETU resource privileges and may lead to disciplinary action in accordance with the SETU disciplinary procedures. Internet postings which are deemed to constitute a breach of this policy may be required to be removed; failure to comply with such a request may result in disciplinary action.

6. Measuring Success

N/A

7. Review of Policy

This policy will be reviewed in advance of the review date i.e. 6 September 2026, and/or as soon as possible following new or updated legislation, national or sectoral policy.

Appendix A

Legislation referenced in the drafting of this policy:

- Copyright Act (1963) and as amended
- Data Protection Act (1988)
- Prohibition of incitement to hatred Act (1989)
- Criminal Damage Act (1991)
- Freedom of Information Act (1997)
- Child Trafficking and Pornography Act (1998)
- General Data Protection Regulations (2016)
- Employment Equality Acts 1998 and 2005