TUS

Ollscoil Teicneolaíochta na Sionainne:
Lár Tíre, An tIarthar Láir

Technological University of the Shannon:
Midlands Midwest

Acceptable Usage Policy

COMPUTER SERVICES

Revision History:

Date of this revision: March 2024	Date of next review: March 2027

Version Number/ Revision Number	**Revision Date**	**Summary of Changes**	**Changes marked**

Consultation History: see Appendix B

Development and Approval Log:

Responsible for:	**Title**
Policy Developer:	ICT Systems Integration Manager
Policy Owner:	VP Campus Services and Capital Development
Recommended by:	TUS Audit and Risk Committee
Approving Authority:	TUS Governing Body
Reference Documents:	

Approval:

Version	**Approved By:**	**Date**
1.0	TUS Governing Body	25.03.2024

This Policy was approved by TUS Governing Body. It shall be reviewed and, as necessary, amended by the University annually. All amendments shall be recorded on the revision history section above.

Date Approved: 25.03.24	**Date Policy to take effect:** 25.03.24	**Date Policy to be Reviewed:** 25.03.27

Document Location:

Website – Policies and Procedures	X
Website – Staff Hub	
Website – Student Hub	
Other – Internal Use Only	

CORPORATE POLICY DOCUMENT

Table of Contents

1. Policy Introduction

The TUS Acceptable Usage Policy outlines the responsibilities of the users of the Technological University of the Shannon (TUS) Information and Communication Technology (ICT or IT) Resources and their interactions with these Resources. It provides information as to the correct usage of the TUS ICT infrastructure and provides guidance on what is and is not acceptable when using the ICT systems, network, devices, services, and software (collectively referred to as TUS IT Resources throughout this document) provided by TUS.

2. Purpose of Policy

The purpose of this policy is to define the requirement for responsible and appropriate use of TUS IT Resources and to provide all those who use TUS IT Resources with clear guidance on the acceptable, safe, respectful, and legal way in which they can use TUS IT Resources.TUS provides IT Resources to users to enable them in performing their duties.

TUS IT Resources will be used only for activities directly associated with the work of TUS. Users are expected to ensure that use of TUS IT Resources is carried out in an acceptable, safe, respectful, and legally compliant manner.

By using any TUS IT Resources, you agree to comply with the terms of this policy. Nothing in this policy affects a person's rights under law.

This policy should be read in conjunction with the Supporting Documentation as outlined in Appendix A.

This Policy is designed to ensure that TUS can offer the widest possible range of IT systems and network resources to TUS users in a way that is compliant with data security and data protection and is not intended to limit use of TUS information services.

3. Definitions

Access: includes access to or using TUS IT Resources from within TUS, and remote access to TUS IT Resources when not onsite at a TUS campus.

CSD: refers to the Computer Services Department, which is the department within TUS that manages access to and administration of IT Resources.

Data Protection Legislation: refers to the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), and the Data Protection Acts 1988 – 2018.

External Parties: any users who are not employees or students of TUS who have a requirement for access to TUS IT Resources and have been granted this access to perform duties for or on behalf of TUS.

IT Servicedesk: initial point of contact for all IT queries in TUS. It can be accessed at https://itservicedesk.midlands.tus.ie/ (TUS Midlands) or https://itservicedesk.midwest.tus.ie/ (TUS Midwest)

Staff: refers to all full-time, part-time and agency employees of TUS.

TUS Data: (including "TUS Master data" and "TUS Transaction data" referred to in this policy) refers to any physical or electronic information stored, processed, or transmitted using TUS IT Resources. "TUS Data" is the sole property of TUS, precluding any infringement of Data Protection legislation.

TUS IT Resources: includes but is not limited to:

- End user devices such as desktop PCs, tablets, laptops, and other devices
- Printers
- Servers
- Software systems and applications
- Network media such as switches and wireless routers
- Network connectivity (TUS Network)
- Smart Phones and other portable devices
- All other media and peripheral devices provided by TUS.
- Cloud applications and services provided by TUS.
- Digital subscription resources provided by TUS.

User: refers to any staff, student, internal (e.g. campus company) or external party who is authorised to use TUS IT Resources and access TUS Data, and who has been given a certain level of access rights (user ID, password, and authorisation levels) in order to do so.

4. Scope

This Acceptable Usage policy covers acceptable usage of:

- TUS Data.
- TUS IT Resources.
- TUS Devices.
- All other TUS information assets.
- Information Systems including but not limited to all infrastructure, networks, hardware, and software, which are used to manipulate, process, transport or store information owned by TUS.

It applies to usage of all computing and networking facilities and devices provided by any Department or Functional area of TUS. It should be interpreted so that it has the widest application.

The TUS Acceptable Usage Policy applies to users of TUS IT Resources.

Policy development, review and approval in TUS is co-ordinated through the TUS Policy Unit, working with the relevant policy stakeholders and policy developers across TUS.

The TUS Acceptable Usage Policy should be read in conjunction with the supporting documentation as outlined in Appendix A

5. Roles and Responsibilities

The following roles and responsibilities apply in relation to this policy:

5.1 Governing Body:

- To review and approve the policy on a periodic basis.

5.2 Vice President for Campus Services and Capital Development:

- To ensure the policy is reviewed and approved by the Governing Body.
- To consult as appropriate with other members of the Vice Presidents/Deans and their Senior Management teams.
- To liaise with Vice Presidents' Offices, Human Resources (HR), or Data Protection Officer (DPO) on information received in relation to potential breaches of the policy. Policy breaches that result in TUS Data being lost/compromised must be alerted to the DPO.
- To ensure the implementation and monitoring of the policy including the development of standards and procedures to support the policy.

5.3 IT Managers:

- To define and implement best practice, standards and procedures which apply to the policy.
- To oversee, in conjunction with data owners, compliance with the policy and supporting standards and procedures.

5.4 Policy Unit:

- To co-ordinate the development, review and approval of this policy, in conjunction with relevant stakeholders and policy developer(s).

5.5 All Users:

- To adhere to the terms of this policy, to include policy statements contained herein.
- To report suspected breaches of policy to their Line Manager/Head of Department and to the IT Servicedesk. Where a violation is of sufficient seriousness, it should also be reported directly to the IT Manager & DPO. Sufficient seriousness in this case refers to policy breaches that constitute compromise or loss of sensitive data, abuse of user privilege, attempted or unauthorised use of another's credentials, or any incident that the Line Manager/Head of Department deems serious enough to alert the IT managers.

6. Policy Statement

Users are required to abide by the law of the State, by this policy, by the Data Protection Legislation and by any additional policies as laid down from time to time, in relation to the proper usage of computer equipment and associated devices.

Use of TUS IT Resources in a manner which contravenes this policy may result in disciplinary action as outlined in Section 7 – Violation of Policy. Violation of this policy can lead to sanctions up to and including suspension or expulsion of a student user, and termination of employment of a staff user. The underlying principle of this policy is that all users are expected to conduct themselves in a professional and appropriate manner (including to always ensure a high level of ICT security awareness) in their use of TUS IT Resources.

Within the setting of TUS, the traditions of academic freedom will be respected. TUS is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination on the grounds of gender, civil status, family status, sexual orientation, religion, age, disability, race or membership of the Traveller community. TUS encourages all users to employ a professional attitude towards their individual working/operating environment, including in the use of TUS IT Resources.

- Users must take appropriate care when handling or sharing sensitive personal data, (their own or that of others), and to ensure that it is shared in a safe and secure manner in line with TUS policy, standards and procedures, e.g. the TUS Password Standard and Encryption Standard.
- No user shall improperly/maliciously interfere or attempt to interfere in any way with information belonging to or material prepared by another user (e.g. but not limited to, sharing your password with others, attempting to gain access to another user's account).
- Similarly, no user shall make unauthorised copies of information belonging to TUS, another staff member, student, or external party. The same conventions of privacy apply to electronically held information as to that held on traditional media such as paper.
- Users agree to abide by all the licensing agreements for software and scholarly resources entered into by TUS with other parties. Users are responsible and accountable for all activities carried out under their username.
-
- Users must not redistribute or transmit information intended for internal use to parties who do not require it for TUS business use.
- Users must store and process TUS Data in compliance with the Data Protection Legislation and all TUS related policies, procedures, and standards. These procedures are available on the TUS website.

In order to protect the interest of all users of TUS IT Resources, system-based controls have been and will continue to be implemented to prevent inappropriate usage[1]. It is expressly forbidden under this policy to intentionally attempt to circumvent these controls.

1 Web Filtering solutions are one example of system based preventive controls.

6.1 General requirements of the policy

Each User of TUS IT Resources:

- Must only use their TUS e-mail system for TUS related activities.
- Must use TUS internal mailing lists appropriately.
- Must ensure that their usage of the TUS centralised printing system (including scanning and copying) is solely for TUS related material.
- Must only forward e-mail messages to others where their role/job appropriately requires them to do so.
- Must be constantly vigilant to the threats to TUS IT Resources and TUS Data, e.g. phishing emails, ransomware, malware and viruses. All suspected phishing/scam/ransomware emails should be reported to the IT Servicedesk. Where an incident is considered sufficiently serious, it should be reported directly to the IT Manager. End users should block offending email addresses from sending emails to their account using the **Block Sender** feature in Microsoft Outlook.
- Must immediately advise CSD of any suspected acts of violation or breach to this policy or breach of TUS IT Resources, including viruses/malware or suspicion of same, by contacting the IT Servicedesk.
- Must respect the legal protections to data and software provided by copyright and licenses.
- Is responsible for their user account and password and the security of their MFA source (normally their smartphone), and all access to their account and the data contained therein. Users are responsible and accountable for all activities carried out under their username.

Users of TUS IT Resources must not:

- Use their TUS email address for any personal correspondences, e.g. registering with airline/travel companies, on-line shopping, social media sites or any other application.
- Write down or share user passwords or IDs, including TUS ID cards.
- Jeopardise the integrity, performance or reliability of TUS IT Resources. Reasonable care should be taken to ensure that resource use does not reduce the level of integrity, performance or reliability of TUS IT Resources, or result in a denial of service to others. (e.g. attempting to gain access to TUS IT Resources other than those areas to which you have permissions).
- Engage in conduct which interferes with or disrupts others' use of shared computing resources and/or the activities of other users, including studying, teaching, research and administration in or for TUS.
- Use TUS's computers to make unauthorised entry into any other computer or network.
- Connect any non-TUS IT equipment to the TUS wired network (including non-TUS devices e.g. laptops, network hubs etc).
- Use TUS IT Resources to inappropriately obtain, store and/or distribute copyrighted material.
- Use TUS IT Resources to infringe intellectual property rights including trademark, patent, design, copyright or other proprietary and/or moral rights.
- Interfere or attempt to interfere in any way with information belonging to or material prepared by another user.
- Make unauthorised copies of information belonging to another user.

- Attempt to gain access to resources or data for which they have not been specifically authorised nor should they attempt to bypass or probe any security mechanisms governing access to the computer systems.
- Use TUS IT Resources to obtain, store and/or transmit confidential TUS information without appropriate authorisation.
- Represent themselves as another person on, or in an effort to gain access to, TUS IT Resources.
- Load unauthorised and/or unlicensed software onto TUS IT Resources.
- Use TUS IT Resources to participate in unsolicited advertising ("spamming").
- Forward electronic mail messages to mailing lists, without the permission of the originator.
- Forward electronic mail messages with large file attachments (i.e. greater than 1MB) to large internal mail distribution lists.
- Obtain/download, store and/or distribute text or images which contain any materials prohibited by law, or material of a pornographic, racist, or extreme political nature, or which incites violence, hatred or any illegal activity.
- Use TUS IT Resources to create, send, post, download, forward, view, store or display offensive, abusive, vulgar, threatening, or defamatory messages, text, graphics, or images or material from whatever source which may put TUS at risk of prosecution, civil action, embarrassment, or loss of reputation. This includes harassment, discrimination, and intimidation of individuals on the basis of Gender, Civil Status, Family Status, Sexual Orientation, Religion, Age, Disability, Race or Member of the Travelling Community.

6.2 Access to TUS IT Resources from off Campus

Many of the TUS IT Resources are available via the Internet. These resources are "cloud" based and can be accessed from any Internet connection. Separately, TUS also provides access (for designated staff) to IT resources which are on premise i.e. they are hosted within TUS's IT infrastructure, via the TUS VPN and/or remote access sessions to the user's PC in TUS. Access to the TUS VPN must only be initiated from a TUS supplied device (e.g. laptop) and never from a personally owned device.

6.3 Use of and security of TUS devices supplied to facilitate working from home

Most TUS staff are in possession of TUS portable devices such as laptops, tablets etc. to facilitate working from home. Whereas staff are permitted to take mobile devices off campus, staff must be always acutely aware of the security (physical and cyber) of the device. The following rules will apply to all staff with TUS supplied devices:

- The device must always be securely held when off campus (i.e., at a staff member's home) and must never be left in an unattended vehicle.
- The device should only ever be used by TUS staff.
- It is imperative that these devices receive regular antivirus updates. TUS staff should follow the instructions issued by the CSD to ensure their device receives regular updates.
- All TUS devices should be encrypted; if you are uncertain as to the state of your TUS devices encryption, please contact the IT Servicedesk.

- Users must contact the IT Servicedesk in the first instance should their device become damaged or stop working, or if there are any issues with it.

6.4 Systems Monitoring

TUS is committed to ensuring robust information security and to protecting users from illegal or damaging actions carried out by groups and/or individuals either knowingly or unknowingly. TUS respects the right to privacy of staff, students, and external parties. However, this right must be balanced against TUS's legitimate right to protect its interests. To achieve its aims in this regard, TUS reserves the right to monitor all TUS IT Resources and TUS Data for operational and security purposes. The TUS architecture is securely designed and includes logging of all information security related events. Examples include user and system logins, successful and unsuccessful access to accounts, email trails, phone calls made etc. Security controls put in place by TUS CSD conduct monitoring of such events on an ongoing basis.

When reviewing the results of any monitoring conducted in accordance with this section, TUS will bear in mind that users may be in possession of certain material for legitimate teaching, learning and/or research purposes. Users will not be disadvantaged or subjected to less favourable treatment as a result of TUS monitoring, provided they exercise their academic freedom within the law and can demonstrate that their teachings, research or qualifications are relevant to material detected and results revealed by TUS monitoring.

Monitoring of activity on or using TUS IT Resources does not impact on the confidentiality of research or other data stored for the purposes of research projects. Any queries relating to the confidentiality of data stored on individual systems as related to the monitoring and logging of system data for operational and security purposes should be raised with the IT managers.

Computer Services will carry out cybersecurity awareness and training exercises 3-4 times per semester to simulate phishing and other attack vectors as part of the ongoing training of users in the risks associated with various elements of working and operating online.

7. Policy Compliance / Monitoring and Review

7.1 Policy Acceptance

By using any TUS IT resources, users agree to comply with the terms of this Policy.

7.2 Violation of Policy

Contravention of any of the above policy can lead to:

- The removal of TUS resource privileges.
- Disciplinary action in accordance with the applicable TUS disciplinary procedure.

Failure of an individual student or member of staff to comply with this policy may lead to the instigation of the relevant disciplinary procedures and, in certain circumstances, legal action may be taken.

Failure of a contractor to comply could lead to the cancellation of a contract.

7.3 Monitoring and Review

This policy will be monitored and reviewed periodically, and at least every three years, to ensure that it is in line with the TUS Internal Control Framework and overall TUS policy and procedures, and that it accurately reflects the legislative and other requirements of TUS in this area.

Appendix A - Supporting Documentation

- TUS Information Security Policy.
- All TUS Polices relating to Data Protection.
- All TUS ICT Standards.
- The HEANET Acceptable Use Policy published by HEANET available at AUP - Acceptable Usage Policy - HEAnet.

The above list is not exhaustive and other TUS documents may also be relevant.

TUS acceptable usage falls under the scope of several pieces of legislation, including but not limited to:

- General Data Protection Regulation.
- Data Protection Acts, 1998 – 2018.
- European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (as amended).
- Criminal Damage Act, 1991(as amended).
- Copyright and Related Rights Acts, 2000 (as amended).
- Electronic Commerce Act 2000 (as amended).
- Prohibition of Incitement to Hatred Act, 1989 (as amended).
- Freedom of Information Act 2014 (as amended).
- Protected Disclosures Act, 2014 (as amended).
- Child Trafficking & Pornography Act, 1998 (as amended).
- Equal Status Act, 2000 (as amended).
- Criminal Justice Act, 2011 (as amended).

Appendix B – Consultation Log

NOTE: TUS Policy Review Committee for the TUS Acceptable Usage Policy consisted of:

- Vice President, Campus Services and Capital Development
- IT Managers, Midlands and Midwest
- ICT Systems Integration Manager
- Information and Compliance Officer
- HR Project Manager

Version Number/ Revision Number	**Consultation Date**	**Names of Parties in Consultation**	**Summary of Changes**
0.1	2/9/2021	ICT Department VP Campus Service and Capital Development VP Finance	Version 0.1 of TUS AUP
0.2	6/1/2023	ICT Department	Changed short form from TUSMM to TUS in line with common usage
0.3	16/6/2023		Formatting and editing based on Policy Unit requirements
0.4	11/09/2023	IT Managers	Review by TUS IT managers, expanded sections on personal use and disciplinary requirements, and on using the Block Email functionality in Outlook to update spam filters
0.5	25/10/2023		Reviewed for consistency of references and extraneous/confusing language.
0.6	21/11/2023	Policy Review Committee review	Changes marked and initial policy finalised

0.7	10/1/2024	Audit and Risk Committee review	Expanded Resources to IT resources throughout doc. Minor corrections for clarity and consistency. Policy Office corrected to Policy Unit, added to Roles and Responsibilities.
0.7	9/2/2024	Privacy Engine - Data Privacy Management Platform & Data Protection Consultancy for GDPR, CCPA, HIPPAA and SOC 2.	Following a review from Privacy Engine there were no amendments to make to the policy from a Data Compliance perspective.
0.8	27/2/2024	Audit and Risk Committee Review	6.7 (p.10) – changed '*from time to time'* to *'3-4 times per semester*'
0.9	6/3/2024	Audit and Risk Committee Review	Definition of IT Servicedesk added to Definitions section, section 3. Guideline sentence added to Item 5.5 6.4 - "direction from a member of TUS Management through the IT Managers" removed, confusing language. Changed to "IT Servicedesk" throughout document Reviewed and corrected punctuation and capitalisation Made date format consistent in Appendix B. Capitalised 'Vice President'

8. Consultation and Communication Plan Detail

Please complete the relevant information below:

IDENTIFIED NEED:

A requirement for TUS to have an Acceptable Usage Policy

STAKEHOLDERS:

All TUS employees and students

PROPOSED TIMELINE FOR CONSULTATION:

July 2023 to November 2023

CONSULTATION GROUP COMPOSITION (REVIEW GROUP) (IF NECESSARY)

TUS VP Corporate Services and Capital Development, IT Manager, TUS Midlands, ICT Systems Integration Manager, IT Manager, TUS Midwest, TUS HR Project Manager, Head of Design in LSAD, TUS Information and Data Compliance Officer

PROPOSED TIMELINE FROM DRAFT TO IMPLEMENTATION:

August 2023 to March 2024

BEST PRACTICE REFERENCES:

LEGISLATIVE REQUIREMENTS / REFERENCES:

APPROVING COMMITTEE/S:

Audit and Risk Committee – review and recommendation to the Governing Body for approval.
Governing Body – Approval

PUBLICATION AND INFORMATION PLAN:

Website, Staff Portal and Functional Managers

MONITOR AND REVIEW PROPOSAL:

Monitor annually, update every three years.