Ollscoil
Teicneolaíochta
an Atlantaigh

Atlantic
Technological
University

Acceptable Usage Policy

Version 1.0

Revision History:

Date of this revision: 13th April 2022	**Date of next review:** 13th April 2023

Version Number/ Revision Number	Revision Date	Summary of Changes	Changesmarked
1.0	13th April 2022	New Policy	

Consultation History:

Version Number/ Revision Number	Consultation Date	Names of Parties in Consultation	Summary of Changes
1.0	N/a		

Approval:

This document requires the following approvals:

Version	Approved By:	Date
1.0	ATU Governing Body	13th April 2022

Quality Assurance:

Date Approved: 13th April 2022	Date Policy to take effect: 13th April 2022	Date Policy to be Reviewed: 13th April 2023
Written by:	IT PSC	
Approved by:	VP Finance and Corporate Services	
Approving Authority:	ATU Governing Body	
Head of Function responsible:	President ATU and President's Nominee	
Reference Documents:	Acceptable Usage Policies of GMIT, LYIT, IT Sligo, and ATU	

Document Location:

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

This Policy was approved by the Governing Body on 13th April 2022. It shall be reviewed and, as necessary, amended by the University annually. All amendments shall be recorded on the revision history section above.

Table of Contents

1. Purpose

The purpose of this policy is to indicate the requirement for responsible and appropriate use of the Atlantic Technological University (ATU) information technology and communication technology (ICT) resources.

ATU provides resources to staff, students, and external parties to assist them in performing their duties. It is envisaged that these resources will be used for educational, research and administrative purposes.

2. 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 Management 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 Human Resources (HR) or relevant senior management members 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 reinforce the policy.
- To oversee, in conjunction with data owners, compliance with the policy and supporting standards and procedures.
- To inform the VP Finance & Corporate Affairs or the VP Academic Affairs and Registrar of suspected non-compliance and/or suspected breaches of the policy and supporting standards and procedures.

HR Office and Office of the VP Academic Affairs and Registrar

- To follow relevant and agreed disciplinary procedures when HR or relevant senior management is informed of a potential breach of the policy (Refer to Section 7).
- To manage the disciplinary process.

Staff /Students /External Parties:

- To adhere to policy statements in this document.
- To report suspected breaches of policy to their Head of Department or the IT Manager.

If you have any queries on the contents of this policy, please contact the local campus IT Manager.

3. Scope

This Acceptable Usage policy covers acceptable usage of:

- ATU information assets and data
- ATU ICT resources

This policy applies but is not limited to the following:

- ATU staff
- ATU students
- ATU external parties

4. Supporting Standards and Procedures

- ATU Information Security policy.
- Existing Regional Campuses Policies, Procedures & standards.

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

5. Acceptable Usage Policy

Conventional norms of behaviour apply to computer-based information technology just as they would apply to more traditional media. Within the setting of ATU this should also be taken to mean that the rights of academic freedom will always be respected. ATU is committed to achieving an educational and working environment which provides equality of opportunity, and freedom from discrimination on the grounds of race, religion, sex, social class, sexual orientation, age, disability, or special need.

ATU encourage all staff, students, and external parties to apply a professional attitude towards their individual working environment, including the use of ATU ICT resources.

Staff, students, and external parties are responsible for their individual user account and password details (Refer to ATU Password Standard).

- No staff, student or external party shall jeopardise the integrity, performance, or reliability of ATU resources. Reasonable care [1]must be taken to ensure that the use of resources does not reduce the level of integrity, performance, or reliability of ATU IT resources, or result in a denial of service to others.

- No staff, student or external party shall improperly/maliciously interfere or attempt to interfere in any way with information belonging to or material prepared by another end user.

- No staff member, student or external party shall make unauthorised copies of information belonging to ATU, another staff member, student, or external party. The same conventions of privacy should apply to electronically held information as to that held on traditional media such as paper.

- Do not redistribute or transmit information intended for internal use to parties who do not require it for ATU business use.

A limited amount of personal usage of ATU resources is acceptable provided it:

- Does not consume more than a trivial amount of resources;
- Does not interfere with department or staff productivity;
- Is not for private commercial gain;
- Does not preclude others with genuine ATU related needs from accessing the facilities;
- Does not involve inappropriate behaviour as outlined above, and;
- Does not involve any illegal or unethical activities.

In order to protect the interest of staff, students and ATU, system-based controls have been implemented to prevent inappropriate usage[2]. It is expressly forbidden under this policy to intentionally attempt to circumvent these controls.

While the above policy statements and principles apply to all types of IT resource usage including email, internet and social media, additional policy statements are provided in Appendices I, II and III to further clarify what constitutes appropriate usages of various ATU IT resources.

6. Monitoring

ATU respects the right to privacy of staff, student, and external parties. However, this right must be balanced against ATU's legitimate right to protect its interests and meeting legal obligations. ATU is committed to ensuring robust information security and to protecting staff, students, and external parties from illegal or damaging actions carried out by groups and/or individuals either knowingly or unknowingly. To achieve its aims in this regard, ATU reserves the right to monitoring of all ATU information resources and ATU data. Any monitoring of ATU data and/or ATU information resources is to ensure the secure, efficient, and effective operations. The monitoring is non-intrusive and does not involve access or reading of content.

The ATU may at any time permit the inspection or disclosure of information held in ATU's systems:

[1] Staff, Students, and External Parties should reference ATU's end user guidelines to ascertain what constitutes reasonable care.
[2] Web Filtering solutions are one example of system based preventive controls.

- When required by and consistent with the law. The ATU evaluates any such action against the precise provisions of the Freedom of Information Act 2014, General Data Protection Regulation 2016/679 and Data Protection Act 1998-2018, Copyright and Related Rights Act 2000, or other applicable law.

- At the written request of a duly authorised person in support of a bone-fide internal investigation instigated under another of the ATU's Policies.

All ATU system activity including internet, email and social media activity is monitored electronically and logged for the following reasons:

- Monitoring system performance;
- Monitoring unauthorised access attempts;
- Monitoring the impact of system changes and checking for any unauthorised changes;
- Monitoring adherence to the acceptable usage rules outlined in this policy.

When reviewing the results of any monitoring conducted in accordance with this section, ATU will bear in mind that academic members of staff, students and external parties may be in possession of certain material for legitimate teaching, learning and/or research purposes. Academic members of staff, students and/or external parties will not be disadvantaged or subjected to less favourable treatment as a result of ATU's 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 ATU monitoring.

7. Violation of Policy

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

Note that; the ATU will fully co-operate with relevant authorities in investigating and prosecuting any illegal access or activity associated with the use of ATU resources or facilities.

8. APPENDICES

Appendix I – General Acceptable Usage Guidance

- IT resources and internet facilities should only be used for legitimate ATU purposes.
- IT resources and internet facilities should never be used in a way that breaches any of ATU's policies.
- Users are provided with a dedicated single sign on (SSO) account. The user is to use no other account on the network. The user should at all times keep the password of this account secure and private. The user takes full responsibility for the use or misuse of this account.
- The contents of all data repositories (mailboxes, disks, PCs, cloud storage, server shares, caches, etc.) operated in the ATU remain the property of the ATU.
- Data repositories are for ATU related storage only, for work, study, research and other approved activities; they are not to be used for personal data storage.
- Any other form of distribution mechanism or Intranet must have prior authorization by the ATU IT Governance Forum.
- Where a user brings their own PC, Laptop or tablet to the University for usage, the user retains full liability for the usage of this device and the legality of its content. Any connection is subject to conditions and such a device may not be connected to the ATU's wired network without prior written permission of the local IT Operations Manager or Senior Technical Officer; a wireless LAN has been provided for this purpose.

Appendix II – Acceptable Usage Rules for IT Resources and Internet Facilities

The following policy strictly forbids users to:

- Bring ATU into disrepute.
- Breach any obligations relating to confidentiality.
- Defame or disparage ATU or other staff, students, and/or external parties.
- Make inappropriate, hurtful or insensitive remarks about another individual or group.
- Harass or bully another individual or group in any way.
- Unlawfully discriminate against another individual or group. It is against the law to discriminate against another on grounds of gender, marital status, family status, sexual orientation, religion, age, disability, race or membership of an ethnic minority.
- Represent yourself as another person.
- Obtain, store and/or transmit confidential ATU information without appropriate authorisation.
- Breach data protection legislation (for example, never disclose personal information about another individual online unless this is done in compliance with the relevant legislation and ATU authorisation).
- Breach any other laws or ethical standards.
- Ignore the legal protections to data and software provided by copyright and license agreements.
- Load unauthorised and/or unlicensed software onto ATU Resources.
- Use ATU IT resources to inappropriately obtain, store and/or distribute copyrighted material including music files and movies. Any such material found will be deleted without prior notification and the user account associated with the download suspended
- Use ATU IT Resources to infringe intellectual property rights including trademark, patent, design and/or moral rights.
- Obtain/download, store and/or distribute text or images which contain any materials prohibited by law, or material of an inappropriate or offensive nature including pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity. Please note that access to certain pornographic sites may be a criminal offence (Child Trafficking and Pornography Act 1998). Any such suspected case will be reported to the Gardai.
- Use ATU computers to make unauthorised entry into any other computer or network.
- Participate in unauthorised activity which results in heavy network traffic and thereby interrupts the legitimate use by others of ATU resources.
- Disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime under the Computer Misuse legislation[3].

Please note the following restrictions and other considerations:

[3] Most computer crime related offences can be found in section 5 of the Criminal Damage Act, 1991 and Section 9 of the Criminal Justice (Theft and Fraud) Offences Act, 2001. The Council of Europe Convention on Cybercrime, which entered into force in July 2004, also provides guidelines for governments wishing to develop legislation against cybercrime.

- The ATU may filter access to certain Internet sites. User may have an expectation that sites with pornographic or adult material and sites involved in copyright infringement will be blocked.
- The ATU may block certain Internet sites from time to time for operational or security reasons; for example, some social networking sites have been blocked for access from Laboratory and library computers.
- Users are warned that under the Criminal Damage Act 1991, computer data is property and it is an offence to
    - Add to, alter, corrupt, erase or move data to another storage medium or to a different location.
    - Attempt to “hack” or gain unauthorised access to a computer, even if data is not damaged in the process”.

Appendix III – Acceptable Usage Rules for Email

- People should actively seek to use the most appropriate means of communication.
- E-mail may not be used for commercial purposes.
- Personal data should be included in the body or contents of an email. Personal data should only be shared securely through One Drive, Teams or in a password protected attachment.
- ATU email communication can only be carried out on the ATU e-mail system, the use of 3rd party email systems to conduct ATU business is strictly forbidden.
- Users are forbidden from forwarding Institute email automatically to 3rd party email systems.
- Users should not participate in the sending or distribution of chain messages, inappropriate or offensive messages, and advertising or in mass mailings of commercial or unsolicited information (SPAM).

- All views and opinions expressed in e-mail are the responsibility of the author. The ATU accepts no responsibility for such content. Users are warned that under the Electric Commerce Act (2000), e-mails are documents in writing rather than informal communications and may be considered as evidence of a contract and be legally binding

- E-mail services is intended as communications mechanisms, not as storage repositories. Users should ensure that important information is not held on the mail platform and that all critical mail and information is copied to a safe location. Computer Services does NOT maintain backups of data held in the mail system.

- Storage limits are set on ATU mail servers. Where these limits are exceeded, mail services will be automatically suspended.

- E-Mail attachments from unknown or unsolicited sources should not be opened. These should be immediately deleted.

- Access to distribution groups such as “All Staff” and “All Students” lists is restricted to selected staff and to the student’s union. These lists are intended for ATU business only. Should any student want to post to these lists, they should forward the relevant message to the Student’s Union for consideration.

- The ATU reserves the right to automate the inclusion of disclaimers to ATU e-mails.

- Do not forward email messages where permission has been withheld by the originator.
- Do not (without prior notification to IT) forward electronic mail messages with attachments to large internal mail distribution lists.
- Do not remove any copyright, trademark or other proprietary rights notices contained in or on the email message.
- Do not use email to enter into legally binding contracts without proper authority being obtained beforehand.
- Do not use BCC to address recipients inappropriately.

Monitoring

- All of the ATU's email resources are provided for business purposes. The ATU maintains the right to examine any systems and inspect any data recorded in those systems.
- In order to ensure compliance with this policy, the ATU also reserves the right to use monitoring software in order to check upon the use and content of emails. Such monitoring is for legitimate purposes only and in compliance with data protection legislation.

Appendices IV – Acceptable Usage rules for Social Media[4]

The policy statements in this appendix deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Wikipedia, all other social networking sites, and all other internet postings, including blogs, wiki's, and discussion boards.

The policy statements in this appendix applies to the use of social media whether during office hours or otherwise and regardless of whether the social media is accessed using ATU IT facilities and equipment or equipment belonging to members of staff or some other party.

The policy statements below are set out under three headings:

- Protecting ATU's interests and reputation
- Respecting colleagues, students and others
- Protecting Intellectual Property and Confidential Information

Protecting ATU's interests and reputation:

- ATU staff should only use official ATU social media sites for communicating with students and external parties which are managed and moderated as outlined in Social Media Management policy. This includes the use of any social media presence related to the distribution of class materials, study aids, provision of feedback to students or any other supports for teaching and learning activities.
- Staff and external parties must not post disparaging or defamatory statements about:
    - The ATU;
    - Its Staff;
    - Its Students; or
    - Others.
- Staff, Students and external parties should also avoid social media communications that might be misconstrued in a way that could damage ATU's interests and reputation, even indirectly.
- Staff, Students and external parties are personally responsible for what they communicate in social media.
- If your affiliation as a staff member, student or external party of ATU is disclosed, it must be clearly stated that the views presented do not represent those of ATU. For example, you could state, *"the views in this posting do not represent the views of Atlantic Technological University "*.
- Avoid posting comments about sensitive work-related topics. Even if you make it clear that your views on such topics do not represent those of the ATU, your comments could still damage ATU's reputation.
- Strive for accuracy in any material you post online.
- If you see content in social media that disparages or reflects poorly on ATU or staff, students or external parties of ATU, you should contact your line manager.

[4] Staff, Students and/or external parties should refer to ATU's Policy for Social Media Management.

Respecting colleagues, students and others:

- Do not post material that could be deemed to be threatening, harassing, illegal, obscene, defamatory, slanderous, or hostile towards any individual or entity.
- Do not post information including personal information related to ATU staff, students and/or external parties without their express permission.
- Do not provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to ATU and create legal liability for both the author of the reference and ATU.

Respecting intellectual property and confidential information:

- Staff, Students and external parties should not jeopardise ATU's business information, confidential information or intellectual property through the use of social media, internet file sharing or internet file storage sites.

- Staff, Students and external parties should avoid misappropriating or infringing the intellectual property of companies and/or individuals, which can create liability for ATU, as well as the individual author.

- Staff, Students and external parties should not use ATU logos, brand names, slogans or trademarks unless approved.

- Staff, Students and external parties should not post any of ATU's confidential or proprietary information without prior written permission.

- Staff, Students and external parties should not post copyrighted material without citing appropriate reference sources or acknowledging copyright accurately.

Appendices V – Specific Acceptable Usage rules for Computer Laboratories

- A user must be in possession of a valid ATU ID card at all times. The user must present this card on demand to any ATU official. Failure to do so may result in a user being refused access to facilities.
- The user shall not in any way, tamper or misuse ATU equipment, either software or hardware. No form of tampering is acceptable. Activities such as installation of unauthorized software, changing screen saver, settings, etc. have an inherent cost to the ATU in terms of technician service time and will be treated as malicious tampering.
- The facilities are for ATU related educational and research use only. The facilities are not available for use on external projects or for work activities not associated directly with courses or the ATU. Facilities may not be used for any form of personal financial gain or commercial purposes.
- Computer laboratories are an expensive and finite resource. Users may not use computers for playing recreational games or for any other leisure or entertainment purpose.
- No food or drinks are allowed in computer laboratories. Smoking in computer laboratories and the ATU in general is similarly forbidden.
- The playing of music in laboratories, other than under supervision as part of a lecture, is strictly forbidden. Where student must play music or audio files as part of their studies, headphones must be used.
- Users may not leave a computer to which they have logged on unattended. Users may not lock out computers for the use of others. Where computers found locked out or logged in but unattended, the user account will be disabled

Appendices VI – Acceptable Usage rules for Wi-Fi Services

The ATU has established provides Wi-Fi services for staff and student usage and for the use of visiting students, staff, researchers, and other visitors.

- Users are instructed to treat the Wi-Fi LAN as a hostile environment. Users should have either personal firewall software or use the firewall software within their operating system.
- Users should ensure their devices are updated with the latest operating system patches.
- Users should ensure their devices have high quality anti-virus software, updated each day from the manufacturer's web site.
- In the event of a user's device showing any symptoms of virus infection, sequestering or disruptive configuration, and this device will be barred from access to the Wi-Fi until such time as the user can demonstrate the issue has been resolved.
- Users requiring assistance to make a connection should call to the ATU's help desks. Although staff will give users advice and instruction on how to connect devices to the ATU network, the responsibility for making this connection is solely the users. Users will be asked at this time to demonstrate that their equipment has been updated and patched and has a recent anti-virus release. ATU staff will not directly carry out any configuration or remedial work on non-ATU equipment.
- All use of the ATU Wi-Fi Services entirely at the users own risk. No claims for damages will be entertained. The ATU is not responsible for personal equipment or its damage when or if attached to any portion of the ATU network.
- Any form of eavesdropping or monitoring of the wireless network and any form of unauthorized access is not permitted and will be subject to disciplinary procedures or criminal investigation.

Appendices VII – Acceptable Usage rules for Software

Under no circumstances may software be installed on ATU equipment unless it has been authorised and correctly licensed.

- All software in use in the ATU must be correctly licensed. On no account is unlicensed software to be used or copied to ATU computers.
- The purchase of software, systems or cloud services must be authorised in advanced by the ATU Software Evaluation Committee. The sourcing of cloud or hosted services will require approval by the Data Protection Office in advance of the ATU Software Evaluation Committee.
- The ATU takes no responsibility for software illegally installed on ATU equipment, in breach of this policy; the responsibility for such breaches lies solely with the individual involved.

Appendices VIII – IT Managers Contact Details

Campuses	Title	Contact Details
Galway/Mayo Campuses	IT Manager	Tel: 091 742731
Sligo Campus	IT Manager	Tel: 071 9305591
Donegal Campuses	IT Manager	Tel: 074 9186145