

University of Limerick

ACCEPTABLE USE POLICY

Version 3.0

Approved by Governing Authority [Jun 2026]

TABLE OF CONTENTS

1. Introduction 3
1.1 Purpose 3
1.2 Scope 3
1.2.1 To whom does the policy apply? 3
1.2.2 In what situations does the policy apply? 3
1.2.3 Who is responsible for ensuring that the policy (and any associated procedures) is implemented and monitored? 3
1.3 Definitions 4
2. Context 6
2.1 Legal and Regulatory Context 6
3. Policy Statements 7
3.1 General Principles 7
3.2 Access and Monitoring 7
3.2.1 Right of access and limited expectation of privacy 7
3.2.2 What is monitored and who has access 7
3.2.3 Why monitoring takes place 7
3.2.4 Access to the content of communications and files 8
3.3 Computing Resources 8
3.4 Account Security and Passwords 8
3.5 Internet Use 9
3.6 Email Use 9
3.7 Software and Licensing 10
3.8 Malware and Phishing Protection 11
3.9 Privacy and Confidentiality 11
3.10 Copyright and Intellectual Property 12
3.11 Removable Media 13
3.12 Remote and Mobile Working 13
3.13 Unacceptable Use 14
3.14 Monitoring and Inspection 14
3.15 Incident Reporting 15
3.16 Consequences of Non-Compliance 15
4. Related Procedures for Acceptable Use 17
4.1 Procedural cross-references 17
5. Related Documents 18
6. Document Control 19

1. Introduction

1.1 Purpose

1.1.1 The University of Limerick (UL) seeks to promote and facilitate the responsible and extensive use of Information Technology (IT) in support of learning, teaching, research, and community engagement. Providing a reliable, secure, and efficient computing and networking environment for Staff and Students depends on the cooperation of all System Users.

1.1.2 This Acceptable Use Policy (AUP) defines the acceptable and unacceptable behaviours expected of all persons who access, use, or interact with University of Limerick information systems, computing resources, networks, and data. It provides clear guidance on the safe, responsible, and lawful use of University IT and Network Resources.

1.1.3 This policy is issued under the authority of the Governing Authority of the University of Limerick and compliance is mandatory for all persons within its scope. It replaces all previous versions of the UL Acceptable Use Policy.

1.1.4 This policy must be read in conjunction with the University's Information Security Policy, and the related ITD procedures referenced in Section 5.

1.2 Scope

1.2.1 To whom does the policy apply?

This policy applies to all persons granted access to University information systems, networks, or data. The following groups are within scope:

- All staff, students, contractors, consultants, visitors, third-party service providers, and any other individuals granted access to University information systems, networks, or data.
- All University-owned, leased, or managed systems and devices.
- Personal devices used to access University resources or connected to the University network.

1.2.2 In what situations does the policy apply?

This policy applies in all situations where University IT and Network Resources are accessed or used, whether on or off campus. Specifically, the policy applies to:

- All UL networks connected to the UL backbone.
- Cloud systems (whether owned, leased, rented, or on-loan) when connected to the UL network directly or indirectly.
- UL-owned or licensed data and programmes, whether held on UL systems or on private systems.
- Data and programmes provided to UL by sponsors or external agencies.

1.2.3 Who is responsible for ensuring that the policy (and any associated procedures) is implemented and monitored?

The **Executive Committee** holds ultimate accountability for information security at the University. The **Director of Information Technology Division** (Director ITD) and the **Chief Information Security Officer** (CISO) hold operational responsibility for the implementation, monitoring, and continual improvement of this policy and its associated procedures, controls, and supporting documents.

System Administrators are responsible for ensuring that they and the systems under their control operate in accordance with the requirements set out in this policy.

The **Information System Owners -** typically Heads of Faculty, Department, or Divisional Directors whose business or academic processes are delivered through the information system — distinct from the IT team responsible for technical operation - are accountable for ensuring the confidentiality, integrity, and availability of Information Systems, the information in that Information System are protected to the appropriate level and that those operating and managing those systems adhere to this policy.

All **System Users** are responsible for compliance with the requirements of this policy.

Please see the Appendix of the Information Security Policy for all roles and responsibilities related to Information Security.

1.3 Definitions

1.3.1 System or Information System: A group of related hardware units, software programmes, and/or business processes dedicated to a single application or business purpose.

1.3.2 System Owner: The Head of the Faculty or Department that utilises a system to perform their day-to-day operations. The System Owner is responsible for the confidentiality, integrity, and availability of information within that system.

1.3.3 System Administrator: The person responsible for the upkeep, configuration, and reliable operation of a computer system or systems.

1.3.4 System User: All students, employees, consultants, contractors, agents, visitors, and authorised users accessing UL IT systems and applications.

1.3.5 Confidential Information: Information classified at a level requiring protection from unauthorised disclosure, including personal data, financial data, research data under embargo, and legally privileged information.

1.3.6 Personal Data: Any information relating to an identified or identifiable natural person, as defined by GDPR Article 4(1).

1.3.7 Multi-Factor Authentication (MFA): A security mechanism requiring two or more independent methods of authentication from separate categories (knowledge, possession, or inherence) to verify a user's identity.

1.3.8 Principle of Least Privilege: The security principle that users, processes, and systems should be granted only the minimum level of access necessary to perform their authorised functions.

1.3.9 Internet: A globally connected network system that uses a suite of communication protocols to transmit data via various types of media, connecting private, public, academic, and government networks through guided, wireless, and fibre-optic technologies.

2. Context

2.1 Legal and Regulatory Context

The University is committed to complying with all applicable data protection, privacy, and information security laws and regulations. The following legislation and regulations are of particular relevance to this policy:

- General Data Protection Regulation (EU 2016/679) (GDPR)
- Data Protection Act 2018 (Ireland)
- NIS2 Directive (EU 2022/2555) — Network and Information Security
- ePrivacy Directive (2002/58/EC) and implementing regulations
- Payment Card Industry Data Security Standard (PCI-DSS), where applicable
- Freedom of Information Act 2014
- Criminal Justice (Offences Relating to Information Systems) Act 2017
- Sector-specific requirements from funding bodies including Science Foundation Ireland (SFI), Health Research Board (HRB), and Irish Research Council (IRC)
- S.I. No. 360 of 2018 (NIS1 transposition)
- Public Service Cyber Security Baseline Standards (Revision 1, 2022)
- NCSC Draft Risk Management Measures (RMM) Guidance, Cyber Fundamentals Framework (CyFun®)
- Code of Practice for the Governance of State Bodies (2016), Higher Education Authority Act 2022, Universities Act 1997
- EU AI Act (Regulation 2024/1689)
- Specific requirements from the Higher Education Authority (HEA) and the Department of Further and Higher Education, Research, Innovation and Science (DFHERIS)

System Users should be aware that breaches of this policy may have legal consequences under the above legislation.

3. Policy Statements

The following sections set out the principles and requirements that govern the use of University IT and Network Resources. Requirements are presented as discrete, unambiguous statements to aid clarity. Each requirement is individually identified by a reference code for traceability.

3.1 General Principles

The following general principles underpin this policy and are observed by all System Users:

- University computing resources are provided to facilitate work as an employee or student and for educational, research, and administrative purposes.
- System Users are responsible and accountable for all activities carried out under their credentials.
- The ability to perform a particular action on a system does not imply that it is acceptable to do so.
- System Users exercise good judgement and act in a manner consistent with the University's values, policies, and legal obligations.
- Academic freedom is fully respected, but this requires responsible and lawful use of the technologies and facilities made available by the University.

3.2 Access and Monitoring

3.2.1 Right of access and limited expectation of privacy

The University reserves the right to access and review any University-owned system, data, service, or account at any time for legitimate operational, security, audit, investigative, legal purposes or to assess compliance with University policies. System users should have no general expectation of privacy in their use of University ICT facilities and should be aware that this applies also to any personal use of University systems or devices that is permitted under this policy.

3.2.2 What is monitored and who has access

Routine monitoring includes system access logs, network traffic, email metadata, application and service use, security events, and the storage and movement of files and their meta-data. The content of communications and files is not routinely monitored, although meta-data pertaining to them may be. The content may be accessed where this is justified for one of the purposes listed above or as per 3.2.1. Access to monitoring information is restricted to authorised staff who require it for those purposes — principally the IT Security Team, and where relevant, Human Resources, the Data Protection Officer, and the University's legal advisers.

3.2.3 Why monitoring takes place

Monitoring is performed to keep University systems and information secure, to ensure systems operate reliably, to meet legal and regulatory obligations, to investigate suspected breaches of University policy or law, and to support the University's audit and assurance activities.

3.2.4 Access to the content of communications and files

Where access to the content of communications, files, or other personal data held in a University-owned account is required, that access is authorised through a documented process (ITD Authorising Access to User Data Procedure), recorded for accountability where personal data are involved. Access will be proportionate to the purpose and no broader than necessary for the purpose.

3.3 Computing Resources

Reference	Requirement
AUP-CR-01	University computing and network resources are provided to facilitate work as an employee or student of the University, and for educational, training, research, and administrative purposes.
AUP-CR-02	Computing and network resources must not be used for commercial or personal financial gain.
AUP-CR-03	System Users must use University IT Resources and Information Assets in a responsible, safe, and lawful manner.
AUP-CR-04	System Users must respect the integrity of computer systems, communication devices, and networks to which they have access.
AUP-CR-05	System Users must respect the integrity of the data to which they have access.
AUP-CR-06	System Users must store and process University data in compliance with the University of Limerick Data Protection Policy and Records Management and Retention Policy.
AUP-CR-07	System Users must use University computing resources in a manner that does not pose a risk to University systems or data.
AUP-CR-08	The ability to perform a particular action on a system does not imply that it is acceptable to do so.

3.4 Account Security and Passwords

Reference	Requirement
AUP-ACC-01	Each System User is assigned individual credentials (username and password) for their exclusive use. System Users must not share their credentials with any other person under any circumstances.
AUP-ACC-02	System Users must not attempt to access accounts, systems, or resources for which they are not authorised.
AUP-ACC-03	System Users are responsible and accountable for all activities carried out under their credentials.

Reference	Requirement
AUP-ACC-04	System Users must set passwords in compliance with the UL Password Standard.
AUP-ACC-05	System Users must enrol in and actively use Multi-Factor Authentication (MFA) for all University systems where it is required.
AUP-ACC-06	System Users must lock or log out of systems when leaving a workstation unattended.
AUP-ACC-07	System Users must not expose their passwords to others or allow them to be visible to third parties.

3.5 Internet Use

Reference	Requirement
AUP-INT-01	Internet access is provided for University business, educational, and research purposes.
AUP-INT-02	Internet access must not be used for commercial or personal financial gain.
AUP-INT-03	University computing resources are provided to facilitate a person's work as an employee or student of the University of Limerick and/or for educational, training, or research purposes. Computing or network resources must not be used for commercial or personal gain.
AUP-INT-04	System Users must not access, download, or distribute material that is illegal, obscene, or in violation of University policy.
AUP-INT-05	System Users must not attempt to bypass internet security controls, web filters, or monitoring systems.
AUP-INT-06	Confidentiality cannot be assured for internet-based communications. System Users must exercise caution when transmitting confidential or sensitive information via internet-based channels.
AUP-INT-07	System Users must not register their University email address on external websites, forums, or email distribution lists, except those that are directly related to University work or educational purposes.

3.6 Email Use

Reference	Requirement
AUP-EML-01	University email is provided for University business purposes. Limited personal use is permitted subject to the conditions in AUP-INT-03.
AUP-EML-02	Email must be treated as formal written communication. System Users must not send, forward, or store messages containing material that is

Reference	Requirement
	offensive, obscene, defamatory, discriminatory, sexist, racist, or otherwise inappropriate.
AUP-EML-03	System Users must not use email for unauthorised mass mailing or commercial solicitation.
AUP-EML-04	System Users must exercise care when handling email attachments. Suspicious emails or attachments from unknown or unusual sources must not be opened and must be reported to the ITD Service Desk immediately.
AUP-EML-05	System Users must exercise care when attaching documents to outgoing emails to ensure that only the correct and intended information is released.
AUP-EML-06	System Users must not read or access email messages addressed to another user, except where explicitly authorised under the ITD Email Management Procedure.
AUP-EML-07	Email messages must not be automatically forwarded or redirected to external non-University accounts.
AUP-EML-08	System Users must not send Confidential or Restricted information via email without appropriate encryption or prior authorisation.
AUP-EML-09	The email system must not be used as the primary means for sending or storing Personal Data. Where Personal Data must be electronically transmitted, secure encrypted alternatives (such as HEAnet FileSender) must be used.
AUP-EML-10	Where personal data is to be sent by email, it must be in a file which is encrypted and password protected using AES (Advanced Encryption Standard) and use a minimum key length of 256 bits or an equivalent encryption strength approved by IT Security.
AUP-EML-11	Email records are subject to the Records Management Policy and Records Classification and Retention Schedule. System Users should periodically delete unwanted emails and empty their Deleted Items folder.
AUP-EML-12	System Users should be aware that email records may be subject to Freedom of Information requests and legal discovery and Data Subject Access Requests under GDPR.
AUP-EML-12	All email accounts maintained on UL email systems are the property of the University of Limerick. UL may access and/or inspect a System User's email in the circumstances described in Section 3.2.

3.7 Software and Licensing

Reference	Requirement
AUP-SW-01	System Users must not install unapproved or unlicensed software on University-owned devices. If you are unsure whether software is approved, please verify with your line manager.
AUP-SW-02	System Users must only use software provided or approved by ITD on University-owned devices.
AUP-SW-03	System Users must comply with all software licensing agreements entered into by the University.
AUP-SW-04	System Users must not copy, distribute, or reverse-engineer University-licensed software.
AUP-SW-05	Software and information provided by the University may only be used for the System User's duties as an employee or student, or for educational purposes.
AUP-SW-06	System Users must not download or install software from untrusted or unverified sources.

3.8 Malware and Phishing Protection

Reference	Requirement
AUP-MAL-01	System Users are expected to verify the authenticity of unexpected or unusual communications, particularly those requesting sensitive information or urgent action.
AUP-MAL-02	System Users are required to complete the mandatory security awareness and phishing training provided by ITD. For more details on those requirements, see the ITD Cybersecurity Awareness & Compliance Procedure.
AUP-MAL-03	System Users must not disable, alter, or uninstall anti-virus or endpoint protection software on University-owned devices.
AUP-MAL-04	System Users must not take actions to prevent or delay the automatic installation of security patches or software updates on University-owned devices.
AUP-MAL-05	System Users must be alert to the possibility of phishing and social engineering attacks and must report suspicious emails or messages to the ITD Service Desk.
AUP-MAL-05	System Users must immediately report any suspected compromise of their credentials, device, or account to the ITD Service Desk.

3.9 Privacy and Confidentiality

Reference	Requirement
AUP-PVY-01	System Users must not access, or attempt to access, information belonging to another user without explicit authorisation.
AUP-PVY-02	System Users must not make unauthorised copies of information belonging to another user or the University.
AUP-PVY-03	System Users are prohibited from transmitting University confidential information via personal email accounts or any unapproved communication platforms.
AUP-PVY-04	System Users must not use University resources to create, publish, or distribute material that is obscene, libellous, defamatory, or in violation of any third party's rights.
AUP-PVY-05	System Users must exercise caution when transmitting confidential or sensitive information via any electronic means. Confidentiality cannot be guaranteed for electronic communications.
AUP-PVY-06	System Users must be aware of and comply with applicable data protection legislation when handling personal data. For further details please see the Data Protection Policy or contact the University DPO directly.

3.10 Copyright and Intellectual Property

Reference	Requirement
AUP-CPY-01	System Users must respect copyright in all software, data, and information accessed through University resources.
AUP-CPY-02	System Users must not infringe any copyright residing in documentation, software, or any other material.
AUP-CPY-03	System Users must comply with all laws as well as University requirements and policies relating to computer use, computer networks, and intellectual property, including applicable data protection legislation.
AUP-CPY-04	System Users must comply with the University's Ethical and Legal Use of Electronic Copyright Material procedure.
AUP-CPY-05	System Users must not make, store, transmit, or make available illicit copies of any copyright material on University systems, equipment, or storage media.
AUP-CPY-06	System Users must not upload, store, or make available unauthorised copies of copyright material via the University's network or internet connection.
AUP-CPY-07	System Users must not use University ICT facilities or systems to obtain, share, store, or distribute copyrighted material without the necessary

Reference	Requirement
	licence or permission, including through file-sharing services, streaming platforms, generative AI tools, or any other means.
AUP-CPY-08	System Users must not duplicate, copy, or make available any material licensed for use within the University to any third party (including their own personal equipment) unless explicitly licensed to do so.
AUP-CPY-09	It is the responsibility of each System User to familiarise themselves with any licence or copyright arrangements applicable to material they use, and to comply with those arrangements.

3.11 Removable Media

Reference	Requirement
AUP-REM-01	Removable media (including USB drives, external hard drives, and memory cards) must only be used where no suitable alternative method of data transfer or storage exists.
AUP-REM-02	Only University-purchased or University-approved removable media must be used for University data. Personal removable media must not be used to store or transfer University data.
AUP-REM-03	Any removable media containing University data must be encrypted in accordance with ITD encryption requirements (see ITD Data Encryption Procedure).
AUP-REM-04	Removable media that is no longer required must be submitted for secure destruction in accordance with ITD procedures.

3.12 Remote and Mobile Working

Reference	Requirement
AUP-RMW-01	System Users may only access University systems remotely through approved remote access solutions provided or authorised by ITD.
AUP-RMW-02	System Users must ensure that any device used to access University resources meets the minimum security requirements defined by ITD.
AUP-RMW-03	System Users must not store Confidential or Restricted University data on personal devices unless explicitly authorised and the device is appropriately secured in accordance with ITD requirements.
AUP-RMW-04	Remote access is provided on the Principle of Least Privilege. System Users will only be granted remote access to systems they are authorised to use.

Reference	Requirement
AUP-RMW-05	System Users must return all University-owned devices and peripherals at the conclusion of their employment, studentship, or contractual relationship with the University.

3.13 Unacceptable Use

The following behaviours constitute unacceptable use of University IT resources and may result in disciplinary action, restriction of access, or referral to law enforcement authorities.

Reference	Requirement
AUP-UNA-01	System Users must not undertake any actions that bring the University into disrepute.
AUP-UNA-02	System Users must not create, exchange, or distribute files or messages that are illegal, offensive, harassing, defamatory, obscene, threatening, sexist, or racist, or that conflict with University policies, the Staff and Student Code of Conduct, Dignity and Respect policies, or national legislation.
AUP-UNA-03	System Users must not connect unauthorised equipment to the University network.
AUP-UNA-04	System Users must not use another System User's account or credentials.
AUP-UNA-05	System Users must not bypass, circumvent, or attempt to defeat any security control, monitoring system, web filter, or access restriction.
AUP-UNA-06	System Users must not engage in any behaviour that poses a risk to the confidentiality, integrity, or availability of University systems or data.
AUP-UNA-07	System Users must not use University systems to conduct any illegal activity, including but not limited to fraud, harassment, or infringement of intellectual property rights.
AUP-UNA-08	System Users must not attempt to exploit, probe, test vulnerabilities, or perform unauthorised network scanning or reconnaissance activities in or from University systems or networks without prior written authorisation from the Head of IT Security.

3.14 Monitoring and Inspection

Reference	Requirement
AUP-MON-01	While the University respects individuals' right to privacy, UL reserves the right to monitor, audit, and inspect all information stored or transmitted on University systems and networks, including internet usage and email, as required for security, policy compliance, legal, or regulatory purposes.

Reference	Requirement
AUP-MON-02	System Users should be aware that the University may retain logs of system, network, or internet access, including the identifier of the computer accessing the internet, the site accessed, the volume of data transferred and the user of the computer. These logs may be reviewed for information security, security monitoring, legal or policy compliance purposes.
AUP-MON-03	Personnel who operate and support internet and email communications facilities may, in the course of their duties, inadvertently observe the contents of electronic communications. Such unavoidable inspection is limited to the least invasive level required to perform those duties.
AUP-MON-04	Systems personnel must not intentionally search electronic communications records for violations of law or policy unless it is a part of their role and they have been authorised or requested to do so.
AUP-MON-04	Systems personnel must report violations of UL Policy or Irish Law which they noticed or discovered inadvertently in the course of their duties.
AUP-MON-05	UL may access and/or inspect a System User's UL email account, UL systems or UL data storage in any of the following circumstances: (a) required by law; (b) substantiated reason to believe that violations of law or University policy have taken place; (c) reasonable suspicion that use of computing resources has caused or could cause reputational damage to the University; (d) required by ITD when dealing with a cyber-incident; or (e) under time-dependent critical operational circumstances. Please see the ITD Authorising Access to User Data Procedure for more details.
AUP-MON-06	Access to a System User's email under the circumstances described in AUP-MON-05 requires the authorisations specified in the ITD Authorising Access to User Data Procedure except in emergency circumstances where the minimum necessary action may be taken immediately.

3.15 Incident Reporting

Reference	Requirement
AUP-INC-01	System Users must report any suspected security event, incident, or policy breach to the ITD Service Desk immediately upon detection.
AUP-INC-02	Reportable events include but are not limited to: lost or stolen devices, suspected phishing or social engineering, unauthorised access, unusual system behaviour, and any suspected compromise of credentials or systems.
AUP-INC-03	Breaches of this Acceptable Use Policy must be reported to the IT Security Team.

3.16 Consequences of Non-Compliance

Failure to comply with University Policies or Acceptable Use Policies, including repeated failure to attend training, undermines the University's efforts to protect data, digital infrastructure, and its compliance with legislation (including GDPR).

Instances of non-compliance may result in restricted access to IT systems and may also be considered as misconduct or serious misconduct under Statute No. 4 of the University of Limerick: Statute on Disciplinary Matters, Suspensions, Termination and Capacity, depending on the severity and risk to the University systems or data.

Persons in contravention of this AUP are subject to the University of Limerick's applicable disciplinary and/or criminal procedures.

4. Related Procedures for Acceptable Use

Implementation of this policy is supported by the following ITD procedures, which provide the operational detail required to give effect to the policy statements set out in Section 3. These procedures are maintained by the IT Division and are referenced throughout this policy.

4.1 Procedural cross-references

- **ITD Email Management Procedure** — governs access to email and email retention (referenced by AUP-EML-06 and AUP-MON-06).
- **ITD Authorising Access to User Data Procedure** — governs access to user data, accounts, and the contents of communications (referenced by AUP-MON-05 and AUP-MON-06).
- **ITD Data Encryption Procedure** — specifies encryption requirements for data at rest, in transit, and on removable media (referenced by AUP-EML-10 and AUP-REM-03).
- **ITD Cybersecurity Awareness and Compliance Procedure** — governs mandatory training and ongoing user awareness (referenced by AUP-MAL-02).
- **ITD User Access Control Procedure** — governs identity, authentication, and authorisation (supports AUP-ACC and AUP-RMW).
- **ITD Privileged Access Management Procedure** — governs access to elevated privileges on University systems.
- **ITD Network Security and Remote Access Procedure** — governs remote access methods (supports AUP-RMW-01).
- **ITD Disaster Recovery Procedure** — supports the availability requirements of this policy.

5. Related Documents

The following University policies, standards, and procedures support or directly relate to this policy:

- Information Security Charter
- Information Security Policy
- Data Protection Policy
- Records Management Policy
- Risk Appetite Statement
- Anti-Fraud Policy
- Intellectual Property Policy
- UL Password Standards
- ITD User Access Control Procedure
- ITD Privileged Access Management Procedure
- ITD Network Security and Remote Access Procedure
- ITD Disaster Recovery Procedure
- ITD Data Encryption Procedure
- ITD Cybersecurity Awareness and Compliance Procedure
- ITD Authorising Access to User Data Procedure
- Staff and Student Code of Conduct
- Statute No. 4 of the University of Limerick: Statute on Disciplinary Matters, Suspensions, Termination and Capacity

6. Document Control

Document Version	3.0
Document Owner	Chief Information Security Officer
Approved by	Executive Committee
Date	20 May 2026
Approved by	Audit & Risk Committee
Date	29 May 2026
Approved by	Governing Authority
Date	16 June 2026
Effective Date	16 June 2026
Scheduled Review Date	16 June 2028