University of Limerick

ACCEPTABLE USAGE POLICY

Contents

1 Introduction

1.1 Purpose

University of Limerick seeks to promote and facilitate the proper and extensive use of Information Technology in the interests of learning, teaching and research, including business and community engagement partnerships.

Providing an efficient and reliable computing and networking service, as well as access to communications devices, to Staff and Students depends on the cooperation of all Users. It is therefore important that you, as a User, are aware of your responsibilities. Whilst the tradition of academic freedom will be fully respected, this also requires responsible and legal use of the technologies and facilities made available to students, staff and partners of the University.

The purpose of this Policy is to provide all Users of the University's IT Resources with clear guidance on the acceptable, safe and legal way in which they can use the University's IT and Network Resources.

This Policy should be read in conjunction with the IT Security Policy. Users must also maintain awareness of and comply with related ITD procedures which include, but are not limited to, ITD User Access Control Procedures, ITD Network Security and Remote Access Procedures, ITD Mobile Device Management Procedures and ITD Disaster Recovery Procedures

1.2 Scope

To whom does the policy apply?

The Acceptable Usage Policy applies to all Staff and Students of the University of Limerick, visitors, contractors, third party agents and all other affiliate associates and users of UL IT and Information assets.

This policy should be read with the University of Limericks Information Security Policy and other supporting policies and procedures.

In what situations does the policy apply?

This Policy applies to the use of the University of Limerick's IT computing resources, including networks, access to the internet, email, computers, laptops, other mobile devices, and any other related software and hardware. Users using personally owned equipment attached to the University's network are also bound by this policy.

This Policy, along with relevant supporting policies, relate to use of all:

- UL networks connected to the UL Backbone
- UL-owned/leased/rented and on-loan facilities.
- Private or cloud systems (whether owned/leased/rented/on-loan) when connected to the UL network directly, or indirectly.
- UL-owned/licensed data/programs, on UL and on private systems.

- Data/programs provided to UL by sponsors or external agencies

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

Within UL, and under the direction of the COOReg, the Information Technology Division (ITD) has overall responsibility for managing the IT resources of the institution.

1.3 Definitions

System or Information System
This is a group of related hardware units, software programs and/or business processes dedicated to a single application or business purpose

System Owner
This is the Head of the Faculty or Department that utilises the system to perform their day to day operations, this system owner is responsible for the confidentiality, integrity and availability of information in the asset in question

System Administrator
This is the person responsible for the upkeep, configuration, and reliable operation of a computer system or systems

System Users
These are students, employees, consultants, contractors, agents and authorized users accessing UL IT systems and applications.

Internet
The internet is a globally connected network system that uses a suite of communication protocols to transmit data via various types of media. The internet is a network of global exchanges – including private, public, business, academic and government networks – connected by guided, wireless and fiber-optic technologies.

2 Context

2.1 Legal and Regulatory Context

2.1.1 ***Data Protection Acts 1988-2018, EU General Data Protection Regulation (GDPR)***

The University is committed to complying with all applicable Data Protection, privacy and information security laws and regulations in the locations in which it operates. In Ireland, the Data Protection Acts 1988 -2018 and the EU General Data Protection Regulation apply to the processing of personal data. Under this legislation, the University is required to take appropriate technical and organisational measures to ensure the safety and security of personal data it processes. In particular, the University is obliged to take appropriate security measures against unauthorised access to or alteration, disclosure or destruction of data and against accidental loss or destruction. Where the University does not take appropriate security measures, it may be acting in breach of legislation

With regard to security measures for personal data, the Data Protection Act 2018 states:

72. (1) In determining appropriate technical or organisational measures for the purposes of section 71 (1)(f), a controller shall ensure that the measures provide a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the data concerned.

(2) A controller or processor shall take all reasonable steps to ensure that—

(a) persons employed by the controller or the processor, as the case may be, and

(b) other persons at the place of work concerned,

are aware of and comply with the relevant technical or organisational measures referred to in subsection (1)"

Article 32 of the EU General Data Protection Regulation states:
"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller, and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"

2.2 Other Context

2.2.1 ***UL's IT Strategy UL Enable 2018 to 2022***

Enabling University of Limerick to Deliver its Mission

UL's IT Strategy, UL Enable 2018 – 2022 was approved in late 2017. UL Enable is focused on creating the IT services and environment whereby the University is 'enabled' to realise its academic mission through the use of technology. UL Enable outlines a 2-stage approach, whereby stage-1 is focused on improving the maturity of the IT Services and environment in UL and stage-2 envisions bringing IT and technology to the fore of strategic planning in the

institution. A key part of stage-1 is ensuring that the IT environment is optimised from an IT security and architecture perspective. Under the umbrella of the IT Strategy, the role of the Head of Enterprise Architecture and Security was created, as was the creation of an IT Security Officer position. With the creation of these positions, there has been an increased focus on IT Governance within UL on areas such as the use of cloud services and the general IT security environment. An IT Security Programme of work that aligns with the UL Enable timeline was started in late 2018. With the increasingly complex cyber landscape and the increased complexity of the legislative landscape, the continuous improvement of the IT security environment is a key focus within the implementation the UL Enable strategy.

*2.2.2 **UL IT Security Governance***

The IT security governance model is the management system by which UL directs and controls IT security and provides oversight to ensure that identified IT Security risks are adequately mitigated. IT Security management ensures that controls are implemented to mitigate identified risks. Security of UL's IT and data assets requires a coherent governance model that ensures that all IT systems in the University are operated in accordance with approved policy and best practice.

IT Security Management

Within UL, the Information Technology Division (ITD) has overall responsibility for leading the IT Security Management objectives of the institution. In order to ensure that IT Security Risks are identified and managed in line with UL's Risk Management policy, ITD has implemented IT security controls and management reporting within the Quality Management System of the IT Division.

As part of ITD's monthly and quarterly Quality Management reviews, IT Security related incidents, events and security related KPIS are measured and reported on. Interventions and controls are implemented where incidents and risks are identified through this management review process. IT Security risks where identified are recorded and managed via ITD risk register. Where the risk rating requires, IT Security risks may be escalated to the fundamental risk register of the University and the University's Risk Management function notified, in accordance with UL's Risk Management Policy.

ITD periodically reports on IT related risks including security risks to the University's Audit and Risk Committee of the Governing Authority.

Enterprise Architecture Review Board

ITD's Enterprise Architecture (EA) Review Board meets periodically to review the nonfunctional aspects of business change and IT projects within UL's IT ecosystem. One of the guiding principles of the EA Review Board is to ensure that changes and IT systems are aligned with good practice from an IT Security and IT Architecture perspective. It is the role of the EA Review board to review new IT initiatives and make recommendations on design and implementation to ensure that IT security and IT architecture are considered from a design perspective and the UL's IT Systems and data are not compromised as a result of new initiatives and projects.

Cloud Governance Group

Cloud services provide significant benefits to individuals and organisations with increased solution choice, flexibility, scalability and faster time to solution. Challenges can arise without the appropriate checks and due diligence, which can lead to significant risks for the University:

- Data Security risks to University of Limerick Data with services that have not been assessed if fit for purpose
- Compliance issues with current UL Data Protection Policy and Regulations
- Contractual issues which may leave UL inadequately protected from a legal or 3rd party contract standpoint

UL has established a Cloud Governance Working Group with appropriate collective expertise to give guidance to UL stakeholders on the use of Cloud Services. The Cloud Governance Group's responsibilities include conducting reviews for approving Cloud solutions to ensure adopted cloud solutions:

- Are aligned with IT Security Best Practices
- Have appropriate data protection provisions
- The SLA's & contracts are fit for service purpose

The Cloud Governance Group meets monthly and proposals to adopt cloud can be submitted and the Group can be consulted for advice and guidance on the existing and proposed future use of industry cloud solutions to address business needs.

*2.2.3 **UL Risk Management Framework***

The UL Risk Management Framework is an iterative process consisting of steps when taken in sequence, enable continual improvement in decision making. It constitutes a logical and systematic method of identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable the University to minimise losses and maximise opportunities.

The University of Limerick Risk Management Framework provides assurance from academic and administrative functions to the senior management team and, through the team, to the Audit & Risk Committee and Governing Authority. Effective risk management focuses on understanding and measuring risk rather than necessarily avoiding or totally eliminating it and comprises the following components:

- Risk Identification
- Risk Assessment
- Risk Monitoring and Reporting
- Risk Appetite
- Risk Management

With regard to Compliance, Regulation and Ethics matters, the University is committed to maintaining the highest standards of integrity, compliance, and ethics. As such the University has **no appetite** for any breaches in statute, regulation, professional standards, research ethics, bribery, or fraud.

*2.2.4 **UL Management Roles and Responsibilities***

The UL Executive Committee

The UL Executive Committee is responsible for supporting the Director of ITD in the enforcement of the Policy where necessary.

Faculty Deans and Directors of Administrative Areas

Faculty Deans and Directors of administrative areas are required to familiarise themselves with the Policy. Where a breach of the Policy is highlighted, faculty Deans and Directors of administrative areas must co-operate in ensuring that appropriate action is taken. Faculty

Deans and Directors of administrative areas are obliged to ensure that all IT systems under their remit are formally administered either by an administrator appointed by the head of an academic and administrative area or centrally by ITD.

The Director of the Information Technology Division

The Director of The Information Technology Division or his/her deputy is responsible for the management of the UL Network and for the provision of support and advice to all nominated individuals with responsibility for discharging these policies.

The Information Security Officer

The Information Security Officer is responsible for:

- Advising the University officers, Administrators, Director of ITD and other appropriate persons on compliance with this Policy and its associated supporting policies and procedures.
- Reviewing and updating the Policy and supporting policies and procedures.
- The promotion of the Policy throughout the University.
- Periodic assessments of security controls as outlined in the Policy and supporting policies and procedures.
- Investigating security incidents as they arise.
- Maintaining records of security incidents.
- Ensuring that IT Security awareness training is promoted and encouraged on an ongoing basis to staff and students of the University. This is to ensure that the necessary precautions are taken at an individual level by stakeholders to protect themselves and the University against the cyber-threat landscape.

Information Systems Users

It is the responsibility of each individual Information Systems user to ensure his/her understanding of and compliance with this Policy. This Policy should be read in conjunction with the IT Security Policy, and users should be aware and familiar with the Supporting IT Security Procedures outlined in Related Documents.

All individuals are responsible for the security of University Information Systems assigned to them. This includes but is not limited to infrastructure, networks, hardware, software and the handling of data. Users must ensure that any access to these assets, which they grant to others, is for University use only, is not excessive and is maintained in an appropriate manner.

3 Policy Statements

- UL will endeavour to ensure that information is created, used and maintained in a secure environment
- UL will endeavour to ensure that computing facilities, programs, data, networks and equipment are adequately protected against failure, loss, misuse or abuse
- UL will endeavour to ensure that all users are aware of and fully comply with the Policy and the relevant supporting policies and procedures
- UL will endeavour to ensure that all users are aware of and fully comply with the relevant Irish and European Community legislation
- UL will endeavour to create awareness that appropriate security measures must be implemented as part of the effective operation and support of Information Security
- UL will endeavour to ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data they handle

4 Related Procedures for Acceptable Usage

4.1 Acceptable Usage

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.

Users must follow any standards and guidelines (including those set out in this Policy) relating to the use of the University's IT Resources and University Information Assets.

- Users must use the University's IT Resources and University's Information Assets in a responsible, safe and lawful manner.
- Users must respect the integrity of computer systems, communication devices and networks to which they have access.
- Users must respect the integrity of the data to which they have access.
- Users must store and process University data in compliance the University of Limerick Data Protection Policy and Records Management and Retention Policy

Software & Licensing

Software and/or information provided by the University of Limerick may only be used as part of the user's duties as an employee or student of the University or for educational purposes.

The user agrees to abide by all the licensing agreements for software entered into by the University.

User Accounts and Passwords

Students and staff are allocated individual accounts to use University computing resources. Each account has a username and password. These are for the exclusive use of the person using computing resources. Unauthorised use must not be attempted to or made of computing or network resources allocated to another person.

The user is responsible and accountable for all activities carried out under his/her username. The password associated with a particular personal username must not be divulged to another person.

Privacy

No user shall interfere or attempt to interfere in any way with information belonging to another user. Similarly, no user shall make unauthorised copies of information belonging to another user. The ability to undertake a particular action does not imply that it is acceptable.

Users must not use any of the University's computing or network resources to make use of, or publish material that is obscene, libellous or defamatory or in violation of any right of any third party.

Normal behaviours that apply to traditional, non electronic media apply similarly to computer based information.

Copyright

Any software, data or information which becomes available through the use of computing or communications resources shall not be copied or used without permission of the University, or any other owner of the software, data or information.

The user must not infringe any copyright residing in documentation of software.

The user must comply with all laws relating to the use of computers, use of computer networks and copyright (in particular the provisions of applicable data protection legislation).

External Access

The user may use approved University of Limerick links to external computing facilities they are authorised to use. When using such facilities, the user must abide by the rules or code of conduct of the host organisation.

The user may use external access to its University of Limerick computing facilities that they are authorised to use. When using such facilities, the user must abide by the ITD Network Security and Remote Access Procedures and the University's Cloud Governance process if hosting University Data on externally owned cloud computing facilities.

4.2 Internet

Internet access is provided to staff and students to enable them to pursue their work as an employee or student of the University of Limerick. The Internet must not be used for commercial or personal gain.

Personal Use

Staff and students may use the Internet for personal use provided that it:

- does not incur additional cost to the University
- does not prevent the employee from attending to and completing work effectively and efficiently
- does not preclude others with work-related needs from using the resources
- does not result in any unauthorised personal profit to the individual
- does not expose the University to legal liability • does not involve or constitute an illegal activity.
- does not expose the University to reputational damage

Confidentiality

Regardless of the level of protection provided for Internet communications, confidentiality cannot be assured. Confidentiality might be compromised, for example, by law or policy, including this Policy, by unintended redistribution, or by the inadequacy of current technologies to protect against unauthorised access. Therefore, users should exercise extreme caution in using Internet communications to transmit confidential or sensitive matters.

4.3 Email

Email Usage

- An email should be regarded as a written formal letter. Any defamatory or careless remarks can have very serious consequences. The use of indecent, obscene, sexist, racist or other inappropriate remarks whether in written form, in cartoon form or otherwise, is strictly prohibited.
- To prevent computer viruses being transmitted through the network, care must be taken when dealing with suspect e-mails and attachments of unknown origin are received. Suspect e-mails should be deleted immediately and never forwarded to other Users.
- Great care should be taken when attaching documents to ensure the correct information is being released.

- Staff and Students are not authorised to retrieve or read any email messages that are not sent to them except when authorised under the approved procedure: ITD Email Management Procedure.
- Email messages must not be automatically forwarded (redirected) to external non-university accounts.

Retention
Email records are considered to be "General Correspondence" under the Records Management and Retention Policy. Where the content of an email and/or its attachment(s) fall under another specific class of record in the Records Retention Schedule, it should be handled, retained and disposed of appropriately as set out in the Schedule.

Users should be aware that is good practice to periodically delete unwanted or unnecessary emails and to empty their Deleted Items folder.

Liability
The nature of email is that there is no guarantee of delivery or confidentially. Therefore the University cannot accept any liability for delivering or for the confidentiality of any message sent from or to the University

Email and Personal Data
The email system should not be used for sending or storing Personal Data. Where Personal Data must be electronically transmitted alternatives such as "HEAnet FileSender" should be utilised as the data can be encrypted and transmitted in a secure fashion.

4.3.1 Ownership and Access

All email accounts maintained on UL email systems are the sole property of the University of Limerick. The University encourages the use of email and respects the privacy of users.

UL can access and/or inspect a User's email in the following cases:
- when required by and consistent with law.
- when there is substantiated reason or suspicion to believe that violations of law or of University policies have taken place.
- when there is reasonable suspicion that the use of the email system has or could result in reputational damage to the University.
- when required by ITD when dealing with or responding to a cyber-incident / event.
- under time-dependent, critical operational circumstances.

When, under the circumstances described above, the contents of electronic communications must be inspected, monitored, or disclosed without the holder's consent, the following shall apply: University staff shall comply with University requests for copies of email records in their possession that pertain to the business of the University, or whose disclosure is required to comply with legislation.

In the situations listed above, UL's IT Department or Data Protection Officer may access an email account with the sole authorisation of the Director of ITD or his/her Deputy or Delegated authority. Such urgent access may be required from time to time (i.e. for example to mitigate risk when dealing with a cyber-threat or event.)

In emergency circumstances the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorisation

Please refer to the ITD Email Management Procedure for more details on Access to other Users Accounts and other procedures for UL email.

4.4 Monitoring

There is a need for systems personnel to inspect the contents of electronic communications and transactional records when redirecting or disposing of otherwise undeliverable electronic communications. Such unavoidable inspection of electronic communications is limited to the least invasive level of inspection required to perform such duties. Systems personnel shall not intentionally search electronic communications records or transactional information for violations of law or policy but shall report violations discovered inadvertently in the course of their duties

Internet Logs

Users should also be aware that the University may retain logs of access to the Internet - including the identifier of the computer accessing the internet, the identification of the site being accessed and the amount of data transferred. These logs may need to be reviewed for information security or other purposes relating to efficient use of University resources.

Unavoidable Inspection

Users should be aware that, during the performance of their duties, personnel who operate and support internet communications facilities (e.g. Internet or Email or Network) need from time to time to monitor transmissions or observe certain transactional information to ensure proper functioning of University internet communications facilities and services, and on these and other occasions might inadvertently observe the contents of internet communications

Privacy Protection

Regardless of the level of protection provided for electronic communications, confidentiality cannot be assured. Confidentiality might be compromised, for example, by law or policy, including this Policy, by unintended redistribution. Users should exercise extreme caution in using electronic communications to transmit confidential or sensitive matters. Users should be sensitive and aware of applicable data protection legislation when using email to transmit confidential or sensitive data.

4.5 Unacceptable Use

The user must not undertake any actions that bring the University into disrepute. Persons in contravention of this Acceptable Usage Policy are subject to the University of Limerick's disciplinary and/or criminal procedures.

The following use of the Internet and Email will be considered a violation of UL AUP Policy:

- The creation and exchange of files/messages that are illegal, offensive, harassing, defamatory, obscene or threatening or that are in conflict with the principles of this Acceptable Usage Policy, University Staff and Student Code of Conduct and Dignity and Respect Policies, or national legislation.
- Connect unauthorised equipment to the University network.
- Use another Users account
- University of Limerick staff and students shall not make, store, transmit or make available illicit copies of any copyright material on University of Limerick systems, equipment or storage media.

- University of Limerick staff and students shall not upload, store or make available unauthorised copies of copyright material via the University's local area network or the internet.
- University of Limerick staff and students shall not assist or participate in any infringement of such copyright materials by operating or connecting to a peer-to-peer network or index using University systems, equipment or data network.
- It is the responsibility of each member of staff and each student to make themselves aware of any licence/copyright arrangements in place and to comply with same before using copyright material.
- University of Limerick staff and students shall not duplicate, copy or make available any material that is licenced for use within the University to any other third party (including the staff or student's home equipment) unless licenced to do so.
- Users must not compromise the privacy of their password by giving it to others or exposing it to public view
- Users must not register their UL email address on external sites, websites, forums or email distribution lists - except those for University related purposes.

Breaches of this policy should be reported to the Director of ITD.
Users in violation of this policy are subject to the University of Limerick's disciplinary and/or criminal procedures.

5 Related Documents

University of Limerick IT Security Policy
University of Limerick Code of Conduct for Employees
University of Limerick Records Management & Retention Policy
University of Limerick Data Protection Policy
ITD Email Management Procedure
ITD Password Rules and Guidelines
ITD Personal Device Procedure
ITD User Access Control Procedures
ITD Network Security and Remote Access Procedures
ITD Mobile Device Management Procedures
ITD Disaster Recovery Procedures
ITD Encryption Guidelines

6 Document Control

Document Version	1.0
Document Owner	Liam O'Reilly, Director ITD
Approved by	Governing Authority
Date	27th September 2019
Effective Date:	30th September 2019
Scheduled Review Date:	27th September 2020