Acceptable Usage Policy for RCSI Computing and Network Systems

RCSI DEVELOPING HEALTHCARE LEADERS WHO MAKE A DIFFERENCE WORLDWIDE

Contents

1. Purpose

Providing an efficient, secure, and reliable computing and networking service, as well as access to communications devices, to Staff, Students, Researchers and Alumni depends on the cooperation of all Users. It is therefore important that you, as a User, are aware of your responsibilities.

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.

By using any of the University's IT and Network Resources, you agree to comply with the terms of this Policy. This Policy is without prejudice to the right to privacy as protected by the constitution and the European convention on human rights.

2. Policy Scope

This Policy covers documentation of policy, procedures, and standards relating to:

- University Information Assets
- University IT and Network Resources

This Policy applies to all Users of the University's IT resources which includes, without limitation, its networks (accessed on site or remotely), business systems and data contained therein, and/or communications devices hereinafter the University's IT resources. This Policy takes precedence over any policies which may be developed at a local level.

3. Policy

Acceptable Use

- You undertake to comply with the provisions of the Data Protection Act and General Data Protection Regulations.
    - If you process (or intend processing) personal data about others on a computer, you are obliged to comply with the provisions of the Data Protection Acts as amended, updated, or replaced from time to time and the University's Data Protection Policy.

    - Users must store and process University data in compliance with the Data Management Policy and the relevant Data Protection Legislation.

- You agree not to engage in any activity that is illegal under national or international law.

- You agree that all activity on the RCSI Network is monitored and audited for breaches to the acceptable usage policy; this includes email, network and internet access and any network traffic transiting between devices and accounts connected to the RCSI networks, either directly or via remote access methods authorised by RCSI.

- Users must use the University's IT Resources and University's Information Assets in a responsible, safe, and lawful manner and to respect the integrity of computer systems, communication devices and networks to which they have access.

- Users agree to adhere to the IT system security standards set by the University that include but not limited to regular password resets where the password adheres to the password policy, regular updating of antivirus and malware software on all devices used on the RCSI network etc.

- 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. See IT Policies on the RCSI VLE (Virtual Learning Environment) and the Staff Portal

Unacceptable Use

- Using IT provided accounts as a business email account or in such a way as RCSI or the RCSI name might be associated with an individual's business or used to promote any individual business. In particular, the account is not intended to be a used as a means of providing professional medical advice, diagnosis, or treatment, or to imply a license to practice or deliver professional advice that is not also supported by state credentialing, licensing, or other independent qualification.

- Using this account to undertake commercial activities or to otherwise further commercial objectives which are not a part of your affiliation with the University.

- Using IT services for non-RCSI related activities such as:
    - Misrepresenting or incorrect association with the University.
    - Impersonating a university employee, affiliate or third party in a manner that does or is intended to mislead, confuse, or deceive others.
    - Registering and using student accounts for non-University related use (Amazon, Netflix, Spotify etc.).

- Other than while performing their duties, knowingly access, download or distribute illegal or inappropriate material, including material that is in any way pornographic, obscene, abusive, racist, libelous, defamatory, or threatening.

- Using RCSI systems to engage in any form of bullying or other behaviour which is illegal or likely to cause harassment to others.

- Use social media to degrade, bully or intentionally offend Staff, Students or other Users or use these tools to bring the reputation of the University into disrepute. Please reference the University's social media Policy for more details.

- Gain unauthorised access to the account, systems, or equipment of any third party - attempts at 'hacking' may result in criminal prosecution in Ireland or elsewhere.

- Use another Users RCSI account or allow others to use your RCSI account for any reason. This includes the provision of your RCSI account information in response to solicited information requests via email or phone.

- Perform any activities which contravene the laws of the State, or the destination country in the case of data being transmitted abroad.

- Infringe the copyright, patent or other intellectual property rights of any person including, by downloading unlicensed software or other unauthorised materials.

- Infringe the data protection or other privacy rights of any person. Please refer to the Data Protection Policy.

- Use of University systems or resources to facilitate plagiarism or cheating in exams or assignments. Please refer to the Plagiarism Policy.

- Access, modify, or interfere with computer material, data, displays, or storage media belonging to the University or another User, except with their permission.

- Connect unauthorised equipment to the University network.

- Load or execute unlicensed software or other material on the University's IT Resources where this is likely to breach the licensing conditions or other Intellectual Property rights.

- Knowingly introduce any virus, malware or other destructive program or device into the University's systems or network. The User should take all reasonable steps to ensure that they do not inadvertently introduce such programs or devices into the systems or network.

- Store sensitive or confidential University data on personal devices or mobile devices without explicit permissions from appropriate approvers. Please refer to the Data Protection Policy.

4. Roles and Responsibilities

- The University IT resources are to support the activities of the University. Personal use of university resources is not advised as access to resources will cease on completion of studies.

- The University reserves and intends to exercise the right to review, audit, intercept, assess and disclose all messages created, received, or sent over the electronic mail system for any purpose. Notwithstanding the University's right to retrieve and read any electronic mail messages, such messages should be treated as confidential and accessed only by the intended recipient. Users of University facilities are not authorised to retrieve or read any email messages that are not sent to them. However, the confidentiality of any message should not be assumed: even when a message is erased it may still be possible to retrieve and read that message.

- The University reserves the right to review, audit, intercept, and assess data stored on any RCSI owned equipment connected to the RCSI network, should there be a need to do so because of a security breach or disciplinary and/or legal actions due a breach of RCSI policies. This includes but is not limited to laptops, desktops, iPads, mobile devices, external storage devices etc.

- RCSI retains absolute discretion to access any data held on the shared services in your name. RCSI may use any data saved within, including email archives, where RCSI is satisfied that such use will benefit the development of the institution's "education and research potential".

- RCSI has provided students with an IT account, email account and system access to assist with the successful completion of their studies. Access to the account, email and all other systems will cease on exiting the university for any reason, including graduation. Please see the RCSI Alumni Email policy relating to access options after graduation.

- Should you have a genuine need to retain access to your OneDrive and email in relation to ongoing research activities, RCSI will assess this need on a case-by-case basis prior to deciding whether to grant such access for a defined period. RCSI retains absolute discretion in this regard. Compliance with RCSI policies is mandatory during this period.

- RCSI has provided students with a laptop to assist them in the successful completion of their studies. The use of the laptop is required for online study, producing, and submitting assignments, and for examinations. It is the student's responsibility to maintain the RCSI laptop and it is also their responsibility to replace it, should it be damaged, lost or stolen. If the student decides, for any reason, they do not want the laptop it must be returned to the University, with all accessories, and in good working condition. If a student withdraws from RCSI before graduation, they must return the laptop upon deregistration, as it is the property of the University.

- Should any RCSI device (laptop, mobile device, smart phone, tablet) provided to students for university business or academic purposes, be lost or stolen, this must immediately be reported to the RCSI IT Department. Should the lost or stolen device contain any PII data this should be reported to the RCSI Data Protection Office.

5. Breaches of Policy

Persons found contravening these regulations will be subject to the University's disciplinary procedure up to and including dismissal, and/or criminal procedures.

6. Supporting Student Policies