ROGER WILLIAMS UNIVERSITY

Acceptable Use Policy [AUP]

Scope

This policy applies to all users of the University technology resources including but not limited to faculty, staff, students, guests, alumni, and third party users of Roger Williams University information technology resources, irrespective of whether those resources are accessed from on-campus or off-campus locations.

This AUP ensures the use of the University's resources supports its educational, research, public service, and administrative missions in the best possible way. Effective support of the University's mission requires complying with relevant legal, contractual, professional, and policy obligations whenever information technology resources are used. Effective support also means that individuals do not interfere with the appropriate uses of information technology resources by others.

This policy broadly covers all of the University's information technology resources – hardware, software, and content; this includes but is not limited to electronic networks, systems, computers, devices, telephones, software, data, files, and all content residing in any of these (referred to as "IT resources"). This policy applies to all digital records of the University and to the information in those records, regardless of the location.

Wireless and Wired Network Access

The use of Information technology resources is restricted to the University's educational and business purpose. Eligible users are provided network authentication credentials to support their business role and educational purpose.

Neither individuals nor units nor departments are permitted to independently deploy network devices that extend the University network, or that secure or isolate parts of the University network, except as approved by RWU IT or as outlined under the provisions of this policy.

Appropriate Email Use

A Roger Williams University assigned email account is an official means of communication between all users and the University. All communications transmitted via email will be consistent with RWU's administrative policies. Sensitive University and personal information will not be sent via email unless specific steps are taken to confirm that the transmission is secure.

All RWU email users are responsible for information sent from their University assigned or shared account. Unawareness of officially sent email will not be accepted as a reason for failure to respond to or comply with any information contained within the message. Email quotas are enforced and therefore regular email management is required to minimize the possibility of delivery failures. Undeliverable messages caused by a full inbox or use of a filter will be considered delivered without further action required on the part of the University.

Confidentiality of Data

Users are responsible for ensuring security-sensitive information [SSI] is processed consistent with University’s Written Information SecurityPolicy, and state and federal laws. Users of University data that contains SSI must not:

- Disclose data to others except as required by their job responsibilities.
- Use data for their own or others’ personal gain or profit.
- Access data to satisfy personal curiosity.

Reports for official or external distribution must be authorized by the responsible office.

Monitoring and Privacy

As a matter of routine system maintenance and compliance, the University may store electronic communications for a period of time. With reasonable and justifiable cause, the University reserves the right to inspect and examine any University-owned or operated communications system, electronic resource, and/or files without prior notice. No inspection or examination of files or information contained therein will be conducted in violation of applicable privacy laws or regulations.

Although the University seeks to create an atmosphere of privacy with respect to information and information technology resources, users should be aware that the use of the University's information resources cannot be completely private.

Bandwidth and Resource Usage

The University continuously monitors technology resources to ensure availability and optimal performance. The University’s’ management will address issues of excessive use and will work with users and relevant administrator to identify, assess, and address issues of excessive use. Bandwidth usage is prioritized based upon network needs that directly serve the University mission, that avoid or eliminate service degradation, and that enables the most effective overall use of technology resources.

Personal Usage

Minimal or incidental employee personal use that is not part of a legitimate University business function is permitted when it is:

- Not excessive
- Does not result in any measurable costs
- Does not interfere with normal business activities.

Personal use must comply with all applicable University policies. Personal use must not violate the law, interfere with the fulfillment of an employee’s University responsibilities, or adversely impact or conflict with activities supporting the mission of the University.

Circumvention of Security Controls

Users must not run, operate, or otherwise configure software or hardware to intentionally spy or allow access by unauthorized users. Users are prohibited from attempting to circumvent or subvert any IT systems, personal privacy space or physical security measures.

For University-owned assets, the removal or disabling of endpoint device management software without prior approval of RWU-IT is considered a breach of this policy.

Software Installation

Information Technology installs software and updates to RWU-owned devices. Removing or disabling of any RWU installed software without prior approval of IT is considered a breach of this policy.

Users who choose to operate and manage software not licensed by the University are responsible for the associated licensing, installation, updates, and security in accordance with this policy.

Software that reaches the end of support life is, by default, not permitted to connect to the University network because security patches are no longer provided by the vendor. If a special exemption is required, this must be requested formally via RWU's MediaTech Service Desk [mediatech@rwu.edu].

Enforcement:

Sanctions for violations of this policy may include the loss of computing privileges and/or other consequences pursuant to the existing student or employee disciplinary procedures of Roger Williams University. Illegal acts involving RWU computing resources may also subject users to law enforcement referral and/or prosecution by local, state and/or federal authorities.

Policy Governance

University management will periodically review this AUP to ensure business requirements and user needs are being met and reserve the right to amend this policy as needed.

Applicability of RWU Policies

This AUP constitutes a living document and intended to work in conjunction with other University policies and procedures – included but not limited to: Written Information Security Plan; Copyright, Legal and Privacy Statement; Electronic Communications Policy; VPN Policy; Wireless Airspace Policy

APPROVED BY:

Roger Williams University Security Advisory Group, 8/19/2021

Standard Number: IT.AUP.V2
Category: IT Acceptable Use Policy
Owner: Information Technology
Effective: 8/30/2021
Revision History: 8/19/2021 Security Advisory Group
Review Date: 8/19/2021