THE
UNIVERSITY
OF RHODE ISLAND

Policy on IT Acceptable Use

Policy Title	**Policy on IT Acceptable Use**
Policy #	07.103.2
Policy Owner	Chief Information Officer
Contact Information	Questions regarding this policy should be directed to the Chief Information Officer at (401) 874-4599
Approved By	Administrative Policy Committee
Effective Date	June 7, 2022
Next Review Date	No later than June 30, 2027
Who Needs to Know About this Policy	All faculty, staff, students, University Affiliates, vendors, and guests of the University, as well as any other parties granted access to University IT Resources.
Definitions	**Confidential University Data**. All University Data that is required to be maintained as private or confidential by applicable law or agreement, or that the University considers and treats as confidential information, whether protectable under law (e.g., trade secrets), or not (other proprietary or sensitive information that the University would not involuntarily disclose except when required by law). **IT Resources**. All computer and telecommunications equipment, software, data, and media, owned or controlled by University or maintained on its behalf. **University Affiliate**. Any individual who is not a faculty member, staff, or student who otherwise has a formal relationship with the University, including but not limited to visiting scholars, visiting students, postdoctoral or other research fellows, professional program participants, adjunct teaching or clinical personnel, volunteers, employees and associates of the URI Foundation and Alumni Engagement, and members of the University of Rhode Island Board of Trustees. Vendors and contractors are not considered Affiliates. **University Data**. All data or information held on behalf of the University, created as a result and/or in support of University business, or residing on University IT Resources, including both electronic and paper records. University Data includes personal data (e.g., personal emails to friends, copies of tax returns) of Users that do not relate to University business but that Users voluntarily choose to transmit or store on IT Resources. **User**. Any individual granted access to University IT Resources.

THE
UNIVERSITY
OF RHODE ISLAND

Statutes, Regulations, and Policies Governing or Necessitating This Policy	University of Rhode Island Policy on IT Endpoint Protection University of Rhode Island Policy on IT Resources
Reason for Policy/Purpose	To protect University IT Resources and to provide guidance and rules for the use of IT Resources at the University of Rhode Island.
Forms Related to this Policy	None

Policy Statement

The computing, digital technology, and digital information resources at the University of Rhode Island support the teaching, learning, research, administrative, public service, and outreach functions of the University. The purpose of this policy is to enable the University to outline the acceptable use of its information systems and set rules to protect The University of Rhode Island and all members of the University community. The University provides IT Resources for the shared and responsible use by members of its community who are, in turn, expected to use them in an efficient, ethical, professional, and legal manner consistent with the University's mission and operational objectives. Inappropriate use exposes the University and its community members to the risk of data loss and unintended disclosure as well as other legal and liability issues.

Within the terms of this policy, acceptable use shall be taken to mean respecting the rights of other digital Users, the integrity of physical and digital assets, pertinent licenses, and contractual agreements, and, where applicable, maintaining compliance with legal and regulatory requirements.

Applicability

This policy applies to all Users of University IT Resources including faculty, staff, students, University Affiliates, and guests and vendors and contactors given access to and permission to use IT Resources in connection with the work they are performing on behalf of the University or in connection with University business. It applies to IT Resources administered centrally as well as those administered by individual colleges or departments; to personally owned computers and to devices connected to all University networks; and to on-campus computers as well as off-campus computers that connect remotely to the URI network.

While this policy applies across the University, individual departments and units may have additional, more stringent, guidelines specific to their unique missions and operational considerations. In any instances of conflict, this policy shall prevail.

Users' Rights and Responsibilities

Users of University IT Resources are granted permission to use those IT Resources that are required to perform University-related activities, including certain computer systems, servers, software and databases, email, and voicemail systems as well as to the internet. As a condition of their use of IT Resources, Users are responsible for knowing and understanding the policies of the University that apply to the appropriate use of University IT Resources and for exercising good judgment in adherence to these policies. Just because an action is technically possible does not mean that it is appropriate or permitted.

General Provisions

University IT Resources are provided for conducting University-related business, including educational and academic pursuits as well as business operations and all Users must comply with applicable University IT Resources and other associated policies at all times.

Users may not use University IT Resources to deprive access to individuals otherwise entitled to access University information, to circumvent University computer security measures, or in any way that is contrary to the University's mission(s) or applicable law.

While the University recognizes the privacy rights and interests of Users as established by applicable law and University policy, all Users, including all University employees (including student employees) or others engaging University IT Resources on behalf of the University should have no expectation of privacy regarding any University Data they create, send, receive, or store on University-owned computers, servers, or other information resources owned by, or held on behalf of University. The University may access and monitor University Data and its IT Resources for any purpose, and at any time, consistent with the University's mission and its operational needs. With respect to personal data that Users voluntarily choose to transmit or store through or with IT Resources, the University will, to the extent feasible, endeavor to respect the User's privacy interests in the information, but Users similarly should have no expectation of complete privacy in such information, which is subject to the same University access and monitoring practices as other University Data.

As members of the University community, Users may not interfere with the activities of others or use a disproportionate share of IT Resources. Examples of inappropriate use of resources include, but are not limited to:

- Sending an unsolicited message(s) to a large number of recipients ("spamming the network").
- Consuming an unauthorized disproportionate share of networking resources (e.g., misuse of peer-to-peer applications).
- Deliberately causing any denial of service, including flooding, ICMP attacks, or the unauthorized automated use of a service intended solely for human interaction.

Additionally, Users may not engage in unauthorized and inappropriate use of IT Resources. Users shall not interfere with the proper functioning of the University's IT Resources or unreasonably interfere with the ability of others to make use of those resources. Inappropriate activities relative to the use of IT Resources include, but are not limited to excess use of these resources, allowing entry to non-public hosts, tampering with security measures, performing any illegal acts through these resources, the violation of others' privacy, or the use of IT Resources to libel, slander, or harass others. See additionally, the University of Rhode Island policy on IT Resources.

All users of University IT Resources, including faculty, staff, students, and University Affiliates as appropriate, must successfully complete annual security awareness training. Additionally, those users who manage sensitive data must also take and pass annual domain-specific training such as FERPA, HIPAA or other relevant training. Users administering systems (generally IT professionals) must also successfully complete annual training in threat detection, mitigation, and recovery strategies as appropriate for the systems they manage.

Confidentiality and Security of Data

Users shall access University Data only to conduct University business and only as permitted by applicable confidentiality and privacy laws. Users may not attempt to access data on systems that they are not expressly authorized to access. Users shall maintain all records containing University Data in accordance with the State of Rhode Island record retention schedules (see https://www.sos.ri.gov/divisions/frequent-filers/records-management) and any University policies on record retention.

Users may not use or disclose Confidential University Data, or any data that is otherwise confidential or restricted, without appropriate authorization.

Users must ensure any individual with whom Confidential University Data is shared is authorized to receive the information. Such data may not be shared with friends, family members, or other University employees who do not have authorized access. Users must also comply with any provisions of vendor contracts or agreements that protect vendor information such as software code and proprietary methodologies.

If a User's office routinely receives requests for Confidential University Data, that office must have a written process in place documenting how these requests are authenticated, reviewed, acknowledged, and recorded. If a User's office receives a non-routine request for Confidential University Data, that request must be authenticated and approved by the User's direct supervisor, unless the request was received by a member of the President's Leadership Council. The authentication, review, and acknowledgement of this request must be recorded by the User's office and maintained per the appropriate retention scheduled.

Confidential University Data must be stored on centrally managed IT Resources, not on local hard drives or portable devices, except and to the extent such centralized storage is prohibited by law or binding agreement. Additionally, Confidential University Data must be encrypted during transmission over a network and must be encrypted while stored. Any employee who becomes aware of the unauthorized disclosure of Confidential University Data or other restricted information of any kind should report the disclosure to the Information Security Office (security@uri.edu).

All computers connecting to a University's network must run security software prescribed by the Chief Information Security Officer as necessary to properly secure University IT Resources. Devices determined by Chief Information Security Officer to lack required security software or to otherwise pose a threat to University IT Resources may be immediately disconnected by the University from a University network without notice.

Users using commercial cloud services must only use services administered by the University.

Email

Users must use only University-provided email accounts to conduct University-related business, including educational and academic pursuits as well as business operations. The use of personal email accounts to conduct University business is prohibited.

The following email activities are prohibited when using a University-provided email account:

- Sending an email under another individual's name or email address, except when authorized to do so by the owner of the email account for a work-related purpose.
- Accessing the content of another User's email account, except 1) as part of an authorized investigation, 2) as part of an approved monitoring process, or 3) for other purposes specifically associated with the account owner's official duties on behalf of University and with express permission from the owner or the Chief Information Security Officer, or, with reference to employee accounts only, the Assistant Vice President for Human Resources.
- Sending or forwarding any email that is known by the User to contain computer viruses.
- Any use prohibited by this policy.

Emails sent or received by Users while conducting University business are University Data that are subject to state records retention and security requirements.

Remote Computing

All electronic devices including personal computers, phones, or other devices used to access, create, or store University IT Resources, including email, must be password protected in accordance with University requirements and passwords must be changed whenever there is suspicion that the password has been compromised. All University-issued mobile computing devices must be encrypted.

All remote access to University IT Resources must be accomplished using the approved University VPN service with multifactor authentication (MFA).

Any Unattended portable computers, phones, and other computing devices must be physically secured.

Should any University Data be created or stored on a User's personal computer or other device, or in databases that are not part of University's IT Resources, this data and these devices are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to University IT Resources

Computer/Network Accounts and Use

No one shall use another individual's access credentials to access University IT Resources unless explicitly permitted to do so by the owner of those credentials or an appropriate University office. Such access may be granted only when necessitated by the efficient conduct of University business and when the person to whom access is granted has similar access to similar non-electronic information. Individuals who obtain access under these conditions may use such access only for the intended purpose for which it was granted and are responsible for policy violations. In the event of any violation of this section of this policy, both the owner of the access credentials and the individual granted access can be held responsible.

Password Management

University-issued or other required passwords, personal identification numbers (PIN), digital certificates, security tokens or similar information or devices used for identification and authorization purposes shall be maintained securely and may not be shared or disclosed to anyone. Each User will be held responsible for all activities conducted using the User's password or other access credentials.

Copyrighted Materials Usage

U.S. law protects copyrighted materials. The University prohibits all employees and students from violating copyright law in connection with their University activities. Copyright violations include reproducing, distributing, or broadcasting copyrighted materials on University IT Resources unless such use is covered by federal fair use guidelines or other copyright law exemptions, or permission has been granted by the copyright owner.

It is reasonable and acceptable for a user to install and use software on a University computer if they are authorized to do so. Sometimes this will involve accepting EULA terms, perhaps as part of a "click through" agreement. Only Users with appropriate signature authority may accept or agree to EULA terms, as long as the contract has been reviewed by the University Office of General Counsel. Users without signature authority may not accept or agree to any EULA that purports to bind the University or the University of Rhode Island Board of Trustees. Any employee agreeing to a contract/agreement, including a EULA, without proper authorization shall be deemed to be acting outside the scope of their employment and may be held personally liable for a contract and any resulting cost or damages incurred thereunder. [Note: In virtually all cases, when the University obtains a license to use software, it will include language in the license agreement specifying that a User's individual acceptance of EULAs will not be effective, either against the University or the User, and that the only binding EULA will be the one approved and signed by a University authorized signatory. Accordingly, Users' obligations when encountering a "click through EULA" in their work is to make reasonable efforts to be sure the University has entered into a software licensing agreement and EULA with the software maker before the User uses the software and "click-accepts" any click-through EULA.]

Personal Use of IT Resources

University Employees: The University provides IT Resources and associated services to employees of the University for business use. Employee personal use that is not part of legitimate University business is permitted when it is not excessive, does not interfere with normal business activities, and when it otherwise complies University policy. Prohibited personal use for employees includes, but is not limited to, political campaigning, solicitation, unauthorized financial gain, or conducting business that has no official relationship with the University. Additional limits may be imposed by a supervisor, appropriate office, applicable University policies, or state laws.

University Students: Student personal use must adhere to the provisions of this policy and to the University of Rhode Island Student Handbook.

Users who choose to transmit or store their personal information through or on IT Resources (consistent with the limitations of this section) should be cognizant of their limited privacy expectations with respect to that information, as described in earlier sections of this policy.

Disclosure

In disciplinary proceedings, the University, at its discretion, may submit results of investigative actions to authorized University personnel, outside legal counsel, or law enforcement agencies. Suspect communications created with University IT Resources may also be subject to Rhode Island's Public Records statutes. In addition, Users may be subject to legally binding demands such as subpoenas and search warrants. Ultimately, it is the University that owns University IT Resources, not the employees who use them.

Inspection of Electronic Information

Information located on University IT Resources is subject to examination, as deemed necessary, to maintain or improve functioning of technology resources, to comply with or verify compliance with federal or state laws, or investigate alleged violations of University policies or federal and state laws.

The University reserves the right for designated technology administrators to access Users' stored information during normal system performance monitoring and maintenance and when investigating cases of computing abuse. Such access shall be approved by the Chief Information Officer in consultation with the Provost or appropriate Vice President, and General Counsel when necessary.

Policy Enforcement

Disciplinary measures for violations are normally applied by the University office or department appropriate to the violation. Violators may be subject to additional sanctions, penalties, or disciplinary actions imposed by the University and are also subject to international, federal, state, and local laws governing interactions that occur on information technology systems and the Internet. The University may restrict or deny access to University IT Resources temporarily or permanently prior to the initiation or completion of disciplinary procedures when it appears necessary to protect the integrity, security, or functionality of the University's IT Resources.

Reporting

Users should report misuse of University Information Resources or violations of this policy.

- Users who believe that their personal safety is threatened should call URI Public Safety, (401) 874-4910.
- For other incidents Users should contact the IT Security Services Office at security@uri.edu
- For reporting "spam" or unsolicited mail, Users should notify the internet service provider (ISP) from which the mail was sent.

THE
UNIVERSITY
OF RHODE ISLAND

Exceptions

Exceptions to the data storage and system ownership requirements of this policy may be needed to support the research, teaching, and service missions of the University. Such exceptions must be made in writing by the Chief Information Security Officer of the University.

Policy Review and Revisions

(Versions earlier than the first policy number may be paper only)

Policy #	Effective Date	Reason for Change	Changes to Policy
Policy #04-1	April 2008	n/a	n/a
07.003.01	August 31, 2021	Updated to reflect changes in use of IT Resources	Updates to reflect changes in the use of IT Resources
07.003.2	June 7, 2022	Scheduled Review	Addition of training requirements; AVPHR added to Email section; written requirements for exceptions.