UNIVERSITY OF RICHMOND

Policy Manual

Policy #:	IRM-2001	**Policy Title:**	Acceptable Use Policy
Effective:	04/28/2020	**Responsible Office:**	Information Services
Date Approved:	04/27/2020	**Approval:**	Vice President for Information Services and Chief Information Officer
Replaces Policy Dated:	2/3/2017	**Responsible University Official:**	Vice President for Information Services and Chief Information Officer

SCOPE:

This policy applies to the University of Richmond and all of its Affiliates. As used in this policy, the term "Affiliates" means organizations or entities in which the University owns a controlling interest or has the right to elect the majority of the entity's governing board.

INDEX:

POLICY STATEMENT:

IRM-2001.1 – Definitions

<u>User</u> – any individual, including but not limited to faculty, student, staff, contractors, visitors; who access and use University information resources or data.

IRM-2001.1 – Policy Statement

1. **Responsible Use of University Information and Computing Resources**

All members of the University of Richmond Community who use the University's computing and network facilities must use them in an ethical, responsible, and legal manner. This means that individuals are personally responsible for their use of these resources. Individuals must be familiar with and follow all University and Information Services policies. An attempt to engage in a prohibited activity is considered a violation whether the attempt is successful or not.

The University's network and computer infrastructure is a critical and finite resource. Community members rely on high availability and good performance in order to accomplish their work. Systems using excessive amounts of bandwidth, causing network disruption, or are deemed to be a security and/or privacy risk may be disconnected from the network or otherwise limited without warning. If the network event is related to faculty research, IS will attempt to contact the faculty member to resolve the issue before taking the resource offline. Information Services may employ automated systems that partition or restrict network bandwidth, protocols, or access either internally or at the Internet gateway.

The University does not monitor or generally restrict the content of material traversing the University's networks or stored on University managed or contracted systems and devices. The University reserves the right to remove or limit access to material posted on University-owned or administered systems and networks when University policies, contractual obligations, or state as well as federal laws are violated. The University provides computers, software, and network equipment for use by the University community. The University retains ownership and reserves the right to add, remove, upgrade, and replace hardware or software on those systems as deemed necessary by Information Services. In those cases where hardware and/or software was obtained by faculty to support their research, Information Services will work with that faculty member to review available mitigations.
Members of the University of Richmond community must:

- Use resources supplied for purposes that are consistent with the business and mission of the University of Richmond.
- Limit personal use of University computing and storage resources to ensure availability of resources for the business and mission of the University.
- Use the University’s computing facilities and information resources, including hardware, software and computer accounts, responsibly and appropriately.
- Respect the rights and property of others.
- Comply with all applicable federal, state, and local laws as well as University policies.
- Comply with all contractual and license agreements.
- Accept personal responsibility for the proper use of individual accounts and all activity associated with them.
- Safeguard equipment entrusted to them.

Members of the University of Richmond may not:

- Share accounts, passwords, or other computer or network authentication. Information Services may grant authorization for group or organization accounts when there is a need. See Computing Accounts at the University of Richmond.
- Use any means to view or intercept data or network traffic not intended for their viewing or use.
- View, copy, disclose, or modify any files or data that do not belong to them, or to which they do not have specific permission.
- Use computing or network resources to harass, threaten, or otherwise cause harm to others.

- Use the University’s computing resources for commercial or personal purposes not related to the University’s business operations, academic, research, and scholarly pursuits.
- Use any IT systems in a way which suggests University endorsement of any political party, candidate, or ballot initiative. This includes e-mailing political messages to any list service maintained by the University which is not explicitly purposed for the posting of political messages.
- Interfere with the proper functioning of the University of Richmond wired or wireless network. In particular users may not perform service denial attacks and users may not install their own network equipment on campus. See the Wireless Access Policy.
- Use University of Richmond IT systems to distribute, produce, publish, and/or sell obscene or illegal content.

2. Information Security and Privacy

The University takes information security and privacy very seriously for all of its members as well as all of its systems.

The University is the owner of all administrative data; individual units or departments have stewardship responsibilities for portions of that data. Information maintained on University systems is a vital asset that will be available only to those who have a legitimate business need to access it in order to conduct University business. The University does not allow the use of administrative data for anything but the conduct of University business. Employees accessing data must observe requirements for confidentiality and privacy, must comply with protection and control procedures, and must accurately present the data in any use.

Members of the University of Richmond community must:

- Read and agree to abide by the University’s Data Security Policy.
- Be personally responsible for the security and usage of any system connected to the University of Richmond network, not owned by the University of Richmond. Find information on connecting your computer.
- Choose passwords that meet University standards and keep their passwords secure. See the Password Policy. Do not use the password that you choose for your University of Richmond accounts with other off-campus services such as social media, streaming platforms, shopping, etc. as the privacy of your password may not be protected outside the University's network.
- Report unauthorized use of your accounts to your supervisor or the Director of Information Security. If you discover a possible security issue related to University systems report the problem immediately by calling 289-8655 or emailing abuse@richmond.edu.
- Use only those computers and computer accounts for which you have authorization. If you need additional privileges or access contact the Help Desk or appropriate system administrator with your request.
- Comply with requests from Information Services. Information Services' staff will conduct periodic security checks on systems and networks. Individuals may be asked to change their password,

upgrade software, apply a patch or perform some other action to improve system security. Non-compliance may result in termination of access.

- When displaying or publishing photos on Web pages or other public forums you have a responsibility not to compromise the privacy of individuals who are identifiable in those photos. As a rule, photo releases are not required for candid photos taken in public areas. However, a page owner or publisher should immediately remove any photo if the subject of the photo objects to its use and requests its removal.

Members of the University of Richmond may not:

- Disguise or attempt to disguise their identity or the identity of their account or the machine that they are using. Users may not attempt to impersonate another person or computing system account. The use of aliases or nicknames associated with your account in systems where those are commonly used is not considered a disguise and is not prohibited.
- Attempt to gain unauthorized access to any account or system.
- Create or use any program or electronic form that collects account names, passwords or personally identifiable information about individuals without the direct knowledge, approval and assistance of Information Services.
- Copy, report or distribute any personally identifiable, sensitive or confidential data or files to which you as a user of University resources are not authorized or gain inadvertent access. Users must report any occurrences to the data owner or to the Director of Information Security.

The foregoing is not an all-inclusive list; the University reserves the right to determine what uses of its equipment and facilities fall within the bounds of the business and mission of the University. Report abuses of information or computing resources to the appropriate Information Services administrator or to epolicy@richmond.edu.

3. E-mail and Other Electronic Communications

E-mail, text messaging, instant messaging, and other applications are used by most members of the University community. However, all users should understand the limitations of privacy and confidentiality related to them. They should not be used for confidential communication or the transmission of sensitive data. See the University's Data Security Policy for additional information.

E-mail messages are written records that could be subject to review with just cause. E-mail records and information in electronic form on central computers can be subpoenaed. Messages that the user has deleted may still exist on system's backup media for weeks or months.

Certain types of e-mail and uses of e-mail or other forms of electronic communications are prohibited; these include chain letters, obscene messages, harassing messages, and unsolicited political messages. E-mail that violates any University policy or is otherwise used for an illegal purpose is prohibited.

All e-mail sent through the University’s systems and networks must accurately show from whom the e-mail originated.

The University may employ automated systems to reduce the amount of unwanted “junk” mail. It is known that this may on occasion reject a valid e-mail.

SpiderBytes should be used for conveying messages to a large number of recipients. SpiderBytes is a message forum for University of Richmond students, faculty and staff to exchange important information regarding University business and campus-wide events. Do not e-mail large lists through Outlook.

4. Observing the Digital Millennium Copyright Act, and Protecting Intellectual Property and Copyright

Copyright is a form of protection of intellectual property provided by the laws of the United States to the authors of original works. Copyright is an issue of particular seriousness because technology now allows the easy copying and transmission of some protected works.

It is the responsibility of all students, faculty, and staff at the University of Richmond to understand and comply with the University’s policy regarding the Digital Millennium Copyright Act. The University's designated agent for notices under the Digital Millennium Copyright Act is the Head of Scholarly Communications in Boatwright Memorial Library. Federal copyright laws also protect the software available for use on computers at the University of Richmond. The software provided through the University for use by faculty, staff, and students may be used only on computing equipment as specified in the various software licenses.

Faculty, staff, or students must not copy or reproduce any licensed software or intellectual property found on University computing equipment, except as expressly permitted by the software license, author, or granting authority. Faculty, staff, and students may not use unauthorized copies of licensed software on University-owned computers.

5. Problem Resolution and Policy Violations

In cases where a member of the University community has allegedly committed a policy violation, broken a law, or is causing harm to the information infrastructure; Information Services may immediately revoke access privileges pending the outcome of a full review of the alleged violation. Whenever possible, the individual will be notified by phone, electronic, campus or U.S. mail of the alleged violation. A representative of the Information Services staff will contact the person to propose a meeting to discuss the alleged violation.

Depending on the nature of the alleged offense, Information Services may contact the appropriate senior University administrator (Director of Human Resources, Dean, or Vice President) or Campus Police alerting them of the alleged violation and conferring on the appropriate next steps. If the problem or issue in question overlaps with another disciplinary or law enforcement process, Information Services will coordinate with the appropriate office or agency. Penalties for illegal activity or serious violations may be as severe as suspension or dismissal from the University or criminal prosecution.

6. Reporting Abusive Incidents, Harassment or Irresponsible Behavior Related to Technology

If you are a victim of abusive incidents related to technology or you become aware of abusive use of University technology resources, report the violation to the Dean of your college, your supervisor, Campus Police, or Information Services at epolicy@richmond.edu. Sending a message to epolicy@richmond.edu will alert a senior member of the Information Services staff to your situation. Keep copies of e-mail messages, a record of the time and date(s) of the occurrence, and all other information related to the incident for investigative purposes.

IRM-2001.2 – Applicable Regulations & Accreditation Standards

SACSCOC *Principles of Accreditation* 10.6 Distance and Correspondence Education

SACSCOC *Principles of Accreditation* 12.5 Student Records

Digital Millennium Copyright Act of 1998

Related Policies:

Information Security Policy

Wireless Access Policy

Data Security Policy

Password Policy

Digital Millennium Copyright Act Policy

Policy Background:

Initial policy approved June 29, 1999

Revised to designate agent for Digital Millennium Copyright Act (DMCA) May 18, 2010

Integrated with Data Security Policy March 13, 2014

Revised for new DMCA agent designation October 2, 2015

Visitor wireless network added February 3, 2017

Minor revisions in March 2020 reviewed by IT Governance Committee and President's Cabinet prior to approval on April 27, 2020.

Policy Contacts:

Vice President for Information Services and Chief Information Officer

Assistant Vice President for Systems and Networks

Director of Information Security

Head of Scholarly Communications