Acceptable Use Policy

This policy provides the terms of use and expectations for all users of Simmons computer and network resources.

Who Is Covered

This policy gives a general outline of the terms of use and expectations for all faculty, staff and students using Simmons's computer equipment and the voice/data/video networks. All eligible persons, including Alumni and other individuals who use computer and network facilities as guests of the University, therefore, are bound by this policy as a condition for using these resources and are expected to follow the guidelines for acceptable use as described below.

What is Included

The technology covered by this policy consists of the University voice, data and video networks and all computer equipment, software, printers, copiers and other peripherals provided for use by the University. In addition, all Simmons-issued or Simmons-licensed passwords, personal identification numbers, and electronic keys are covered. These resources are the property of or are licensed by the University and are made available for use to Simmons students, faculty, staff and guests as a privilege. Computers owned by individuals but used for school or University-related work are not subject to these use restrictions, except in regards to their connection to or access of the Simmons network or use of University-licensed software or resources.

Nothing in these policies limits or removes the right of free speech or the academic freedom of faculty, staff, and students engaged in educational or scholarly pursuits, nor relaxes responsibilities as members of the Simmons community.

Acceptable Uses

Simmons's technology (computer and network) resources are intended for educational, scholarly and university business uses. Examples of acceptable uses are:

- Coursework and course management
- Thesis preparation and research projects
- Independent research and self-teaching projects
- Communication with students, faculty, and staff at other academic or research institutions
- Communication within and outside the University for educational and for purposes related to the business of the University.

While it is acceptable for students to use University network resources for personal or recreational purposes such as to play computer games or to use chat rooms or personal email, academic work and University business always has priority. In a general access computing environment, if nearby terminals are busy, staff or other users may ask you to relinquish recreational use for academic use, and recreational users are expected to courteously comply.

Technology resources are shared: faculty, staff, and students depend on borrowers of Simmons equipment and media to return them on time and in good condition. Borrowers must return equipment borrowed from Technology on time or pay overdue fees. Technology will

refer to the Office of Student Affairs, students who repeatedly keep equipment past its due date and time. Borrowers may be responsible for the replacement cost of equipment returned in poor condition.

Prohibited Uses

Prohibited uses of Simmons's network and computer facilities include those uses which: infringe on another individual's right to privacy; adversely affect the user community inside or outside of Simmons; violate federal and state laws (including but not limited to laws governing copyright, privacy and harassment); violate Simmons policy; or are not allowed under the terms of our software licenses. Additional examples of prohibited uses include, but are not limited to:

- Unauthorized reading, copying, or modification of files, network traffic or electronic mail other than your own.
- Unauthorized use of someone else's password or sharing of passwords.
- Intentional damage or disruption to hardware, software, services, security devices or codes, or the intentional creation or distribution of viruses, worms or other forms of electronic mayhem.
- Unauthorized access via the voice/data/video network to computers or network traffic at other locations or tampering with the University network or hardware services. [1]
- Abuse of printing privileges, including printing of excessive copies or in violation of copyright.
- Distributing obscene or abusive messages or other forms of harassment.
- Commercial activities, such as selling of personal property, development of software for sale, work undertaken to support any company or other contracted work, unless specific prior authorization is granted.
- Placing excessive demands on network or server capacity.
- Obtaining, storing, using, or sharing copyrighted material (software, text, images, sounds or video in electronic form, etc.) without proper credit to and permission from the copyright owner.
- Revealing confidential information obtained from administrative data systems or otherwise to unauthorized people or groups.
- Unauthorized use of file-sharing software or other applications or equipment that creates excessive network traffic or attempts to circumvent network security or management systems.
- Allowing unauthorized access to the Simmons network through any computer, modem, or network device (including wireless access points).
- Establishing or maintaining a server without specific prior consent of Technology.
- Failure to return borrowed equipment within the loan period.
- Losing or damaging borrowed equipment.

For its own protection, the University reserves the right to block all Internet communications from sites that are involved in extensive spamming or other disruptive practices, even though this may leave University computer users unable to communicate with these sites.

[1] Mass 201 CMR17.04(4)

Passwords and Other Keys

All passwords, pass codes, keys, and personal identification numbers issued to access computer and network resources or University premises are the property of Simmons or are licensed by the University for specific purposes. You are not permitted to use any such tools to access, store or retrieve any information on computer and network resources unless specifically authorized. Without regard to whether information on any resource (such as e-mail, voice-mail, or document files) is access-protected, you may not access any information on any resource maintained by or licensed to another user unless properly authorized by appropriate Simmons personnel or by the user at issue.

Intellectual Property

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors, inventors, trademark owners, and publishers in all media. It encompasses respect for the right to acknowledgment, rights of privacy and publicity, and right to determine the form, manner, and terms of publication and distribution of one's work.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer and network environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

Further information on file sharing, intellectual property rights, and copyright can be found in separate policy documents on each of these subjects.

Installation of Software

Before any software can be used on Simmons computers or the network, the software must be virus-tested; you are prohibited from disabling University-installed virus protection software. No copy of software may be used on the University's computer or network resources unless a valid license to use that copy has been obtained, including shareware and software downloaded from the Internet. You are not permitted to make additional copies of any software without express authorization and proper registration of the copy.

It is illegal to make unauthorized copies of software. Copyright laws protect software authors and publishers, just as they protect authors of printed material. Simmons does not condone the use of illegally copied software and will not provide assistance and support to users of such software. Use or distribution of unlicensed software is not only against University policy, it is also illegal.

Any software installed by individual users must be consistent in intent and practice with the Acceptable Uses outlined above.

Privacy Concerns

The Simmons computing and network resources are the property of the University and under its administration and management. Use of these resources is intended primarily for educational, scholarly and university business purposes. While technical staff and administrators will not casually or routinely monitor traffic content or search files, the University reserves the right to scan all network traffic and devices, as well as review any

information stored or transmitted on this equipment, without notice and notwithstanding any password. These systems shall not be considered private, and discretion will be used when sending and storing highly sensitive or confidential information. Users agree to provide access for encrypted files (subject to mutually agreed confidentiality provisions) to allow the review provided for to take place.

Failure to Comply

Failure to comply with these guidelines for acceptable use of computer resources or other relevant University policies may result in fines or loss of privileges and could include restitution to the University or contracted vendors. Serious or multiple infractions may cause the user to be denied access to University equipment, services and resources, such as workstations, servers, printers and file servers, databases and network access. Repeated instances of copyright infringement will lead to the termination of all user privileges.

Moreover, failure to comply with these policies, particularly where non-compliance results in the violation of federal or state law may expose the user to criminal and civil liability. Certain kinds of computer hacking, computer abuse, and computer-related fraud are not only against this policy; they are illegal and punishable by fines, imprisonment or both. A copy of 18 U.S.C. §1030 et seq., Fraud and Related Activity in Connection with Computers, is available from the University Counsel. The University may report suspected criminal conduct to the appropriate authorities.

Simmons reserves the right to deny an account or access to anyone who has violated the user agreement or fails to pay required fees (including tuition) for network connections, services or accounts as described above. The terms and conditions for usage are subject to change as computing resources and user demands vary.

To protect the owner and others, Technology may need to suspend network access to computers believed to be causing problems until the offending machine has been verified by the Service Desk to be running properly. Because of the impact on others, network access may have to be revoked without notice.

Under unusual circumstances and in violation of these policies, a user may be immediately disconnected from University services.

Adjudication

The Chief Information Officer will receive notice of allegations of violations of this policy. Subsequent to receipt of notice, the Chief Information Officer (or at the discretion of the Senior Vice President for Finance & Administration) will, with the University Counsel, investigate the allegation and make a recommendation of action to the Senior Vice President for Finance and Administration. Sanctions for violations of the policy may include temporary or permanent suspension of computer and/or network user's privileges, as well as the sanctions specified above, in the section entitled "Failure to Comply."

The Senior Vice President for Finance and Administration retains the discretion, subject to review by the President, to suspend permanently the user privileges of any individual who has repeatedly violated this policy or whose sole violation is, in the judgment of the Senior Vice President for Finance and Administration, sufficiently serious to merit permanent suspension of user privileges.

Allegations of misuse of the computer resources may also lead to sanctions pursuant to established University policies and procedures. These policies and procedures are set forth in

the following publications:

- Employee Handbook (employees)
- Student Handbook (students)
- Faculty Policy Manual (faculty)

Allegations of copyright infringement made against a Simmons student, faculty, or staff member are subject to the procedures established by the Digital Millennium Copyright Act. These procedures include notice to the alleged infringer; disabling access to the allegedly infringing material; and, in some cases, re-enabling access to such material, in accordance with the provisions of the Act.

Updates

This policy will be reviewed and updated on a regular basis and users will be publicly notified of any changes.

Contact Information

For further information, contact Technology at Simmons at 617-521-2222 or via electronic mail at servicedesk@simmons.edu

---

Update 09/28/2018
Approved 10/09/2018