The Rockefeller University

Policy on Responsible Use of University Technology Resources

The Rockefeller University Policy on Responsible Use of University Technology Resources

Policy Statement

University technology resources are powerful tools that are made available to support the university's research and education missions and its administrative and other business functions. These technology resources also serve to enhance and improve robust, open communication among and between members of the community and others.

Users of university technology resources ("users") are responsible for exercising good judgment when using these resources, and are expected to be mindful of and respectful towards members of the community and the university. Users should take personal responsibility for adhering to the university's standards of appropriate conduct and propriety. These standards, at an individual level, include the commitment to a professional work environment in which all individuals are treated with respect and dignity and do not experience discrimination or harassment. On an institutional level, these standards include a recognition that university technology resources are provided to support the university's research and education missions, and that misuse of these resources is damaging to the community of individuals who comprise the university and threatens the efficiency and integrity of the university's operations.

Definitions

The following definitions apply to terms used throughout this policy.

- **University Technology Resources** – University technology resources include email, telephone, voicemail, computer hardware and software, Internet access, and the campus computer network and their components or peripheral parts (including computers, telephones, wires, radio, or electromagnetic, photoelectronic, photo-optical, or cloud systems).
- **Electronic Communications and/or Materials** – Electronic communications and/or materials relating to university business and/or to using university technology resources or university facilities or services are defined as any and all data or information in any form (including but not limited to telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage) that is maintained, communicated or posted by any means, including, but not limited to, worldwide web, electronic mail,

bulletin boards, instant messaging or other electronic tools, using university technology resources.

Security of University Technology Resources

The University's Information Technology Department continually takes steps to safeguard the integrity of university technology resources and to maintain and ensure proper operations. To this end, the university has routine monitoring processes (i) designed to manage the type or volume of incoming or outgoing electronic mail, telephone voice mail, or internet usage, (ii) that are not targeted to monitor or intercept the electronic mail, telephone voice mail, or internet usage of a particular user, and (iii) that are performed solely for the purpose of computer system maintenance and/or protection.

The university does not routinely inspect the content of an individual user's electronic communications, and/or materials maintained, communicated, or posted using university technology resources (as defined above), although the university reserves the right to perform monitoring or inspection on an exceptional basis, at any and all times and by any lawful means. Users are advised against any expectation of privacy or confidentiality in such electronic communications or materials. Exceptional circumstances under which the university will monitor, inspect, or take other appropriate actions include, but are not limited to, the following:

- While performing routine security or maintenance functions, Information Technology personnel may detect evidence of a violation of law, university policies or rules, university contractual obligations, or university standards of conduct or propriety, as described more fully below, which will be reported to the university's Chief Information Officer for appropriate action.

- The university may monitor, copy, confiscate, limit, or deny access to, or take other appropriate action regarding the use of university technology resources and/or regarding electronic communications and materials using university technology resources when the university determines that the law, university policies or rules, university contractual obligations, or university standards of conduct or propriety may be violated and/or to investigate credible evidence or allegations of such violations. When a violation has been established, the university will take appropriate action concerning continued use of university technology resources and discipline of employees, up to and including dismissal.

- If the university is notified of a claim of copyright infringement, the university reserves the right to expeditiously remove the allegedly infringing electronic communication(s) and/or material(s) until the claim is resolved. In appropriate circumstances, the university will terminate a user's access to the university's technology resources if the user is found to have repeatedly infringed the copyright of others.

- The university reserves the right to refuse e-mail and other connections from outside hosts that send unsolicited, mass, or commercial messages, or messages that appear to contain viruses, worms, or other malware (i.e., malicious software designed to infiltrate or damage a technology or other electronic system) sent to university or other users. The university reserves the right to disconnect without notice from its networks or other university technology resources, any computer or electronic device that may have a harmful virus, worm, or other malware.

- The university may disclose or otherwise use electronic communications and materials to comply with a subpoena or other legal demand, or to cooperate with law enforcement or federal, state, or local authorities, or in litigation or other legal proceedings.

Responsible Use of University Technology Resources

Users who are provided access to the university technology resources must assume responsibility for their appropriate use. The university expects users to be careful, honest, responsible, and civil when they are using university technology resources.

1. Access to university technology resources is provided for use in support of the university's research, education, administrative, and other business functions. Incidental and occasional personal use of these resources consistent with university policy and rules is permitted so long as such use does not disrupt or distract from the conduct of university business, due to volume or frequency.

2. Users assume personal responsibility for the use of their accounts and are responsible for maintaining the security of their accounts, including their passwords. Passwords on all computers and software applications on campus (including those not maintained by the IT Department) must follow the current university guidelines at: https://it.rockefeller.edu/passphrase#policy

3. Users assume personal responsibility for protecting their computers. Protection from malware, such as viruses and spyware, must be installed according to the university guidelines at: https://it.rockefeller.edu/anti-virus-malware

4. Users assume personal responsibility for proper physical use of the network and must not install inappropriate network devices (such as wireless access points, hubs, and routers) according to the university guidelines at: https://it.rockefeller.edu/network-requirements

5. Users should respect the shared nature of the university's technology

resources and refrain from activities that will interfere with the ability of others to use those resources, including excess usage of bandwidth.

6. Users may not send electronic communications or materials that do not comply with the university's standard of conduct and propriety described in the Policy Statement above. In considering whether an electronic communication or material may be inappropriate, a user should consider whether the content, style, or timing of the communication or material would be perceived as hostile or unwelcome by any recipient or would be unlawful if made public (including through the media or in a court proceeding) and/or if the author was publicly identified.

7. University technology resources may not be used for purposes that violate the law, university policies or rules, or university contractual obligations.

8. Confidential information, particularly medical information or personal or private data typically thought to be non-public (such as an individual's social security number or academic record), must be used and maintained according to applicable law, university policies, rules or guidelines, and university contractual obligations regarding the use and maintenance of such data. Persons who handle this type of material as part of their job duties must follow applicable operating procedures for working with the information.

9. University employees may gain access to confidential or proprietary information through contractual arrangements entered into by the university. Users of university technology resources must not knowingly violate university contractual obligations that restrict the use or maintenance of such information.

10. Use of university facilities, including university technology resources, for commercial activity for personal financial gain is strictly prohibited. This prohibition does not include use of these resources for permissible external activities by investigators pursuant to the university's Conflict of Commitment Policy.

Policy Violations – Examples

Violations of this Policy may occur in a variety of ways. Examples of improper use of university technology resources include, but are not limited to:

- To harass, threaten, or otherwise cause harm to a specific individual(s) or class(es) of individuals, whether by direct or indirect reference, by sending communications that are perceived as hostile or unwelcome, whether of a sexual or other nature, or that reflect bias or disrespect based on race, color, religion, sex, age, national origin, citizenship status, marital status, sexual orientation, military status, veteran status, or disability;

- To download, use, distribute, post, or disseminate material in violation of the law, including but not limited to software infringement; breaking into or tampering with computer systems; unlawful spreading of computer viruses, worms, or other malware; unlawful use or distribution of copyrighted material (e.g., music and movies); defamation or libel; pornography; prohibited gambling and/or theft; or assisting others in any such violations;

- To download, use, distribute, post, or disseminate material, in violation of license restrictions or university contractual agreements;

- To impede, interfere with, impair, or otherwise cause harm to others, including, but not limited to, knowingly propagating electronic chain mail, spamming, electronically misrepresenting the user's or his or her electronic identity (e.g., email spoofing), electronic eavesdropping, or launching a computer virus, worm, or other malware;

- To forge, falsify, alter, or otherwise misuse university or non-university records, including electronic mail headers, electronic directory information, or other electronic information identified as university records, including account, login, or password information; and

- To damage or otherwise interfere with university facilities or resources.

Reporting a Violation or Making Inquiries

If you believe that a violation of this policy has occurred, or you have questions about this policy, contact the Chief Information Officer. The Chief Information Officer will notify other officers and/or university personnel, as appropriate. If you believe that a personnel-related violation of this policy has occurred, or you have personnel related questions about this policy, contact the Vice President for Human Resources.

Effective Date

This Policy is effective on April 6, 2005, upon approval by Frederick M. Bohen and was amended, effective on April 20, 2006, April 12, 2007, December 16, 2016, May 9, 2022, and by Administrative Working Group on January 22, 2024. This Policy may be amended from time to time by the university's Chief Information Officer, Anthony Carvalloza, with the concurrence of the President's Office, or by Administrative Working Group.

Person Responsible for this Policy:

Mr. Anthony Carvalloza
Chief Information Officer