ROSEMAN UNIVERSITY
OF HEALTH SCIENCES

COMPUTER AND NETWORK ACCEPTABLE USAGE POLICY

Approved by Administrative Council 12/10/18

Effective date 12/10/18

PURPOSE

Roseman University of Health Sciences technology resources are intended to support and enhance the academic mission and administrative functions of the university. This Acceptable Use Policy (AUP) states the rules and regulations regarding the use of these technologies. This AUP complements and supplements, rather than replaces other policies concerning appropriate conduct of employees and students of Roseman University of Health Sciences. Roseman's technology resources includes any computer, computer-based network and supporting infrastructure, computer peripheral, e.g. printer, operating system, software or any combination thereof, owned or licensed by Roseman University of Health Sciences or under the custody or control of Roseman University of Health Sciences. This policy also applies to any of the above mentioned items which fall under company and/or personal ownership, used in conjunction with any portions of the Roseman University of Health Sciences networked infrastructure. The university grants access to its networks and computer systems subject to certain responsibilities and obligations set forth herein and subject to all local, state, and federal laws. Appropriate use should always be legal, ethical and consistent with the university's mission, policies, and procedures.

AUTHORIZED USE

Authorized use of Roseman's technology resources is use consistent with this policy. An authorized user is any person who has been granted authority by the university to access its technology resources and whose usage complies with this policy. Unauthorized use is strictly prohibited. The term "user" hereinafter refers to any student, employee, or anyone affiliated with the Roseman University of Health Sciences.

PRIVACY

Users must recognize that there is no guarantee of privacy associated with their use of Roseman's technology resources. The university may find it necessary to view electronic data and it may be required by law to allow third parties to do so (e.g. electronically stored data may become evidence in legal proceedings.) It is also possible that messages or data may be inadvertently viewed by others.

INDIVIDUAL RESPONSIBILITIES

Common Courtesy and Respect for Rights of Others

All users are responsible to respect and value the privacy of others, to behave ethically, and to comply with all legal restrictions regarding the use of electronic data. All users are also responsible to recognize and honor the intellectual property rights of others. Actions or language that constitutes unlawful harassment, threats, intimidation, defamation, or violence are not permitted. Users who engage in such activity will be subject to disciplinary action.

Responsible Use

All users are responsible for refraining from all acts that waste Roseman's technology resources or prevent others from using them. Each user is responsible for the security and integrity of information stored on his/her personal computer. Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with or used by others.

All users must maintain confidentiality of student information in compliance with the Family Education Rights and Privacy Act (FERPA) of 1974, and patient information in compliance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Permitting Unauthorized Access

All users are prohibited from running or otherwise configuring Roseman's technology resources to intentionally allow access by unauthorized users.

Termination of Access

Whenever a user ceases being a student or employee, or if such user assumes a new position and/or responsibility within the university community, such user shall not use facilities, accounts, access codes, privileges, or information
for which he/she is not authorized in his/her new position or circumstances. This includes the return of all Roseman's technology resources including hardware, software, and peripherals when requested.

Attempts to Circumvent Security

Users are prohibited from attempting to circumvent or subvert any security measures implemented for the Roseman's technology resources. The use of any computer program or device to intercept or decode passwords or similar access control information is prohibited.

Denial of Service

Deliberate attempts to degrade the performance of Roseman's technology resources to deprive authorized users of access to or use of such resources is prohibited. This includes the downloading and uploading of illegal files while on the university's network. While the university does not look at the content of an individual's network traffic, Technology Services does monitor bandwidth utilization and can isolate and identify any user who utilizes significant bandwidth for prohibited activities.

Harmful Activities

The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software, or data belonging to the university and the like.

Use of Licensed Software

No software may be installed, copied, or used on Roseman's technology resources except as permitted by the owner of the software and by law. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to.

Taking Equipment Off Campus

There are legitimate circumstances when it may be necessary for employees to take university equipment home, for a period of time, to facilitate the completion of a specific job assignment. Equipment that is permitted to be taken home includes tablets and laptops that have been issued to the employee. Any other equipment requested must be approved by the Vice President for

Technology Services and/or their designee, and must follow the equipment check-out process through the Technology Services Help Desk. Employees may use the approved university equipment at home provided the employee accepts full responsibility for any loss or damage to the equipment if the university's insurance and/or manufacturer warranty does not cover it. The equipment must be returned to Roseman when its use at home is no longer necessary, authorized, or when the employee terminates employment. Failure to do so may result in appropriate sanctions brought against the employee, and they may be responsible for any replacement costs.

In the event that a student's Roseman issued computer will be under repair for longer than 1 (one) calendar day, the student can check out a loaner laptop to take home to ensure their academic demands are not interrupted. Students may use the approved university equipment at home provided the student accepts full responsibility for any loss or damage to the equipment if the university's insurance and/or manufacturer warranty does not cover it. Students must follow the equipment check-out process through the Technology Services Help Desk. The loaner laptop must be returned upon completion of their repaired laptop.

Notice of Digital Millennium Copyright Act (DMCA)

In October 1998, the Digital Millennium Copyright Act (DMCA) was passed. It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works.

Roseman University of Health Sciences requires employees, students and affiliates utilizing University infrastructure to comply with all U.S. copyright laws. Roseman reserves the right to remove or restrict access to materials posted on University-owned equipment if it is alleged that U.S. copyright laws have been violated. If Roseman determines that U.S. copyright laws have been violated, the infringing material will be permanently removed.

Because the DMCA requires copyright holders to notify Roseman if a user has illegally downloaded content, employees, students and affiliates who utilize their computing privileges to misuse the bandwidth for illegal downloads and file sharing will face the following disciplinary actions:

First Offense:

If a complaint is filed against a student, employee or affiliate, the Vice President for Technology Services, or his/her designee, will contact them by e-mail. This e-mail will include the following details of the alleged infringement:

1. The accusing party
2. The name of the file allegedly being shared illegally
3. Other pertinent information

After the e-mail has been sent out, the student, employee or affiliate will have no more than forty-eight (48) clock hours to respond stating that you have removed the file from your computer and/or are no longer distributing it to others, or if you believe that the filed complaint is erroneous. If the Vice President for Technology Services, or his/her designee, does not receive this response within

the designated response time, the student, employee or affiliate's Internet access will be temporarily disabled and a fee of $100.00 will be assessed.

For employees, additional disciplinary action may also be taken by the unit/college/program head and/or Human Resources unit. For students, offenses will be considered a violation of professional conduct and handled accordingly. For students enrolled in dual degree programs, the program director/dean of both academic units will be notified. For employees, the Office of Human Resources and the individual's unit head will be notified.

Second Offense:

If a complaint is filed against a student, employee or affiliate, the Vice President for Technology Services, or his/her designee, will contact them by e-mail. This e-mail will include the following details of the alleged infringement:

1. The accusing party
2. The name of the file allegedly being shared illegally
3. Other pertinent information

After the e-mail has been sent out, the student, employee or affiliate will have no more than forty-eight (48) clock hours to respond stating that you have removed the file from your computer and/or are no longer distributing it to others, or if you believe that the filed complaint is erroneous. If the Vice President for Technology Services, or his/her designee, does not receive this response within the designated response time, the student, employee or affiliate's Internet access will be temporarily disabled and a fee of $250.00 will be assessed.

For employees, additional disciplinary action may also be taken by the unit/college/program head and/or Human Resources unit. For students, offenses will be considered a violation of professional conduct and handled accordingly. For students enrolled in dual degree programs, the program director/dean of both academic units will be notified. For employees, the Office of Human Resources and the individual's unit head will be notified.

Third Offense:

As an administrative action, in order to maintain compliancy and protect the Roseman University of Health Sciences under the DMCA, the student, employee or affiliate's networking privileges can be terminated. As a disciplinary matter, the Vice President for Technology Services, or his/her designee, will refer the matter to unit/college/program head. Students can also be reported to the Student Professionalism Board for additional review. To restore network privileges, the student, employee or affiliate will be asked to sign an agreement with the university, and will be assessed a fee of $500.00.

For employees, additional disciplinary action may also be taken by the unit/college/program head and/or Human Resources unit. For students, offenses will be considered a violation of professional conduct and handled accordingly. For students enrolled in dual degree programs, the program director/dean of both academic units will be notified. For employees, the Office of Human Resources and the individual's unit head will be notified.

Receiving a single DMCA complaint or none at all, does not preclude you from receiving a pre-litigation letter, or being sued directly.

To report suspected copyright infringements occurring on the university's network, please contact the Technology Infrastructure Manager.

Personal Business, Political Campaigning, and Commercial Advertising

Roseman's technology resources are university-owned resources and business tools to be used only by authorized persons for university business and academic purposes. Except as may be authorized by the university, users shall not use Roseman's technology resources for: compensated outside work and/or the benefit of organizations not related to the university, except in connection with scholarly pursuits (such as faculty publishing and approved consulting activities); political campaigning; commercial or personal advertising; or personal gain or benefit of the user.

Using Portable Devices and Removable Media

Users will not copy or store university confidential information on personal removable media or portable devices such as devices, personal digital assistants (PDAs), cell phones, CDs, thumb drives, external hard drives, etc., unless specifically required to do so.

Employees understand and agree that Roseman University has the right to:

- Require the use of encryption devices.
- Implement encryption and apply the other necessary security controls (such as an access PIN and automatic locking) on any mobile device that synchronizes Roseman data regardless of it being a Roseman or personally owned device.
- Remotely "wipe" any synchronized device at the request of that employee if it has been lost or stolen.

Support and Use of Personal Computer Equipment

Technology Services does not provide support for equipment and software that is not university-owned, and will not install or provide software licensed to the university. Such actions would violate the terms of the agreement between software vendors and Roseman University.

Anyone accessing confidential information on personal computer equipment are required to safe-guard their devices with the following:

- Up-to-date anti-virus software
- Password/passcode/PIN to access your device
- Enabled screensaver/screen lock for inactivity to activate after 5 minutes or less of inactivity and require Password/passcode/PIN to unlock it.
- Up-to-date operating system software, e.g., Windows and iOS Updates

Users are advised to not access confidential information in public areas, e.g., airports, restaurants.

Definitions

- Confidential Information: Information that is deemed confidential by the university, a third-party organization or agency, or by law. This includes HIPAA, FERPA, personnel, and finance information.

- Personal Computer Equipment: Devices you own and manage, whether or not you receive a university stipend for them. They include personal computers, laptops, smartphones, tablets, media players, and removable media that can be readily transferred from one electronic device to another.

SECURITY

System Administration Access

The Vice President for Technology Services, or his/her designee, will be granted authority to access files for the maintenance of the systems, storage or backup of information, or pursuing system problems. Further, the university may access usage data, such as network session connection times and end-points, CPU and disk utilization, security audit trails, etc. Such activity may be performed within the reasonable discretion of the Technology Resources division management, subject to approval by the President.

PROCEDURES AND SANCTIONS

Responding to Security and Abuse Incidents

All users have the responsibility to report any discovered unauthorized access attempts or other improper usage of Roseman's technology resources. If a security or abuse problem with any Roseman's technology resources is observed by or reported to a user, such user shall immediately report the same to Technology Resources division management.

Range of Disciplinary Sanctions

Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of Roseman's technology resources access privileges, disciplinary action, monetary fines, and dismissal from the university. Some violations may constitute criminal offenses, as defined by local, state, and federal laws and the university may prosecute any such violation to the full extent of the law.

_____ _____

Printed Name ***Signature***

_____

Date