California Health Sciences University

CHSU ACCEPTABLE USE OF TECHNOLOGY
POLICY FOR EMPLOYEES

I. PURPOSE

A. The purpose of this policy is to ensure a safe and appropriate environment for all employees. This policy identifies the acceptable ways in which University Technology may be used. The University recognizes and supports advances in technology and provides an array of technology resources for employees to use to enhance student learning, facilitate resource sharing, encourage innovation, and to promote communication. While these technologies provide a valuable resource to the University, it is important that employees' use of technology be appropriate to support the University Mission.

II. UNIVERSITY TECHNOLOGY

A. The University provides Information Technology resources and resources to faculty, students, staff and others solely for the purposes of supporting teaching, learning, scholarship, service and administration within the context of the University's mission.

B. University Technology include all electronic technology used to store, copy, transmit, or disseminate visual, auditory, and electronic information as well as the information contained therein. This includes, but is not limited to, computers, tablets, networks, phones, fax machines, copiers, PDAs, cell phones, postage machines and the information contained in them.

III. ACCEPTABLE USE

A. University employees are only permitted to use University Technology for purposes which are safe (pose no risk to students, employees or assets), legal, ethical, do not conflict with their duties or the mission of the University, and are compliant with all other University policies. Usage that meets these requirements is deemed "proper" and "acceptable" unless specifically excluded by this policy or other University policies. The University reserves the right to restrict online destinations through software or other means. Additionally, the University expressly prohibits:

1. Using University Technology for commercial gain;
2. Accessing University Technology for the purpose of gaming or engaging in any illegal activity;
3. Transmission of confidential information to unauthorized recipients;

4. Inappropriate and unprofessional behavior online such as use of threat, intimidation, bullying, or "flaming";

5. Viewing, downloading, or transmission of pornographic material;

6. Using University Technology for the creation or distribution of chain emails, any disruptive or offensive messages, offensive comments about race, gender, disabilities, age, sexual orientation, religious beliefs/practices, political beliefs, or material that is in violation of workplace harassment or work place violence laws or policies;

7. Engage in unlawful use of University Technology for political lobbying;

8. Significant consumption of University Technology for non-business related activities (such as video, audio or downloading large files) or excessive time spent using University Technology for non-business purposes (e.g. shopping, personal social networking, or sport related site);

9. Knowingly or carelessly performing an act that will interfere with or disrupt the normal operation of computers, terminals, peripherals, or networks, whether within or outside the University Technology (e.g., deleting programs or changing icon names) is prohibited;

10. Infringe on copyright, licenses, trademarks patent, or other intellectual property rights;

11. Disabling any and all antivirus software running on University technology or "hacking" with University Technology.

B. Incidental personal use of Information Technology services and resources, within the guidelines of this policy, is considered appropriate. Such permissible incidental personal use does not include hosting, ASP (Application Service Provider), ISP (Internet Service Provider), WSP (Wireless Service Provider) or other services for third parties. Incidental personal use does not include activities for financial gain unless such activities are authorized under University Policy. Incidental personal use does not include the use of institutional data which may be contained in or extracted from institutional computing and communications systems. Personal use is not incidental if it incurs a direct cost to the University.

C. Use of Information Technology services and resources by students, in support of approved experiential learning and/or in support of their duties as compensated employees is explicitly authorized, so long as such usage does not violate any part of this policy.

IV. SECURE USE

A. Users of Information Technology services and resources are responsible for taking appropriate steps to safeguard University and personal information, as well as University facilities and services. Users are prohibited from anonymous usage of University Technology. In practice, this means users must sign in with their uniquely assigned University users ID before accessing/using University Technology. Similarly, "spoofing" or otherwise modifying or obscuring a user's IP Address, or any other user's IP Address, is prohibited. Circumventing user authentication or security of any host, network, or account is also prohibited.

B. Passwords used with University Technology must follow the following standards:

1. Passwords and other authentication and authorization codes, cards or tokens assigned to individuals must not be shared with others. Authorized Users must not provide access to unauthorized users. Passwords should be chosen carefully to lessen the possibility of compromise. Users are responsible for all activity that takes place under their User ID(s).

    1. Passwords must be at least 8 characters long and contain at least one upper case and one lower case letter as well as a numeric value or a special character (!,$,#,%).

    2. Passwords will be changed according to IT Department guidelines.

    3. All computer systems connected to the University network will be configured to lock the screen after a period of 15 minutes of inactivity. All students, faculty, and staff must lock their screen whenever stepping away from their computer.

    4. Activity that may compromise the system integrity or security of any on or off-campus system is prohibited. This includes any type of unauthorized access or hacking.

    5. Unauthorized monitoring of individual User activity, information and communications is prohibited. See the University IT Confidentiality Policy.

    6. Users must ensure the security of restricted, confidential, proprietary, licensed, copyrighted or sensitive information entrusted to their care or that may come into their possession. Security includes, as appropriate, protection from unauthorized disclosure, modification, copying, destruction or prolonged unavailability. Unless approved by the IT Systems Administrator, users must not

store non-university personal identification numbers including, but not limited to, Social Security Numbers, Credit Card Numbers, or Driver's License Numbers on unsecured devices or media, for any period of time.

V. VIRUS SCANNING SOFTWARE

A. The University maintains virus scan software on all systems managed by the University. No system may be connected to the University network without currently updated, Enterprise Class, virus scan software running on the system. Disabling of virus scan software on University technology is prohibited.

VI. PATCH MANAGEMENT

A. The University maintains a patch management system designed to keep all systems connected to the University network up to date with the latest vendor security patches and updates. Users of University systems may, from time to time, be required to present their system for manual updates. All systems connecting to the University network must be updated regularly with vendor security patches and updates.

VII. RESPONSIBILITY

A. Users are responsible for their own use of University Technology and are advised to exercise common sense and follow this Agreement in regard to what constitutes appropriate use of University Technology in the absence of specific guidance.

VIII. RESTRICTION OF USE

A. The University reserves the right, at any time, for any reason or no reason, to limit the manner in which a User may use University Technology in addition to the terms and restrictions already contained in this Agreement.

IX. THIRD-PARTY TECHNOLOGY

A. Connecting unauthorized equipment to the University Technology, including the unauthorized installation of any software (including shareware and freeware), is prohibited.

X. PERSONALLY OWNED DEVICES

A. If an employee uses a personally owned device to access University Technology or conduct University business, he/she shall abide by all applicable University policies, administrative regulations, and this Agreement. Any such use of a personally owned device may subject the contents of the device and any communications sent received on the device to disclosure pursuant to a lawful subpoena.

XI. UNIVERSITY BRANDING

A. Users are prohibited from using the logos, word marks or other official symbols of the University without authorization from the Office of Marketing & Communication. This specifically includes any such usage in connection with electronic systems, services and communications, both internal and external. This does not include the usage on physical or electronic letterhead when used for official University business.

XII. REPORTING

A. If an employee becomes aware of any security problem (such as any compromise of the confidentiality of any login or account information) or misuse of University Technology, he/she shall immediately report such information to their immediate supervisor.

XIII. CONSEQUENCES FOR VIOLATION

A. Violations of the law, University policy, or this Agreement may result in revocation of an employee's access to University Technology and/or restriction of his/her use of University Technology and/or discipline, up to and including termination. In addition, violations of the law University policy, or the Agreement may be reported to law enforcement or other agencies as deemed appropriate.

XIV. RECORD OF ACTIVITY

A. User activity with University Technology may be logged by System Administrators. Usage may be monitored or researched in the event of suspected improper University Technology usage or policy violations.

XV. BLOCKED OR RESTRICTED ACCESS

A. User access to specific Internet resources, or categories or Internet resources, deemed inappropriate or non-compliant with the policy may be blocked or restricted. A particular website that is deemed "Acceptable" for use may still be judged a risk to the University (e.g. it could be hosting malware), in which case it may also be subject to blocking or restriction.

XVI. NO EXPECTATION OF PRIVACY

A. Users do not have any expectation of privacy in their use of University Technology. Log files, audit trail and other data about user's activities with University Technology may be used for forensic training or research purposes, or as evidence in a legal or disciplinary facilitate maintenance, inspection, updates, upgrades, and audits, all of which necessarily occur both frequently and without notice so that the University can maintain the integrity of University Technology. All data viewed or stored is subject to audit, review, disclosure and discovery.

B. Pursuant to the Electronic Communications Privacy act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by University Technology for sending or receiving private or confidential electronic communications. System Administrators have access to all email and will monitor messages. Messages relating to or in support of illegal or inappropriate activities will be reported to the appropriate authorities and/or University personnel.

C. The University reserves the right to monitor and record all use of University Technology, including, but not limited to, access to the Internet or social media, communications sent or received from University Technology, or other uses within the jurisdiction of the University. Such monitoring/recording may occur at any time without prior notice for any legal purposes including, but not limited to, record retention and distribution and/or investigation of improper, illegal, or prohibited activity. Employees should be aware that in most instances, their use of University Technology (such as web searches or emails) cannot be erased or deleted. The University reserves the right to review any usage and make a case-by-case determination whether the User's duties require access to and/or use of University Technology which may not conform to the terms of this policy.

- Policy Owner: Human Resources
- Effective Date: 6/30/2017
- Revised Date: 6/30/2017
- Approval by President Date: 6/30/2017