Information Technology Services - Acceptable Use of Technology

Purpose

The purpose of this policy is to ensure a safe and appropriate environment for all students. 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 students 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 students' use of technology be appropriate to support the University Mission.

University Technology

The University provides Information Technology resources and resources to the members of the CHSU community solely for the purposes of supporting teaching, learning, scholarship, service and administration within the context of the University's mission.

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.

Acceptable Use

University students are only permitted to use University Technology for purposes which are safe (pose no risk to students, students 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 harassment, discrimination, retaliation or violence laws or University 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.

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.

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

Secure Use

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.

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).
2. 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 (!,$,#,%).
3. Passwords will be changed according to IT Department guidelines.
4. All University-owned 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.
5. 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.
6. Unauthorized monitoring of individual User activity, information and communications is prohibited. See the University IT Confidentiality Policy.
7. 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.

Social Media Use

CHSU understands that social media can be a fun and rewarding way to share your life and opinions with family, friends and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. It is now easier than ever to publish and deliver content electronically, while making it practically impossible to permanently erase that content. This means that any content can be published without the filter of time for thoughtful reflection, and can be done so in anger, in sadness, in joy, and perhaps just in error. As health care students and professionals, employees and staff of a center of higher education, we will often be held to a higher standard than the

community at large. Therefore, any negative content associated with us could be amplified in the eyes of the public. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media. This policy applies to all CHSU employees, students, vendors, and third parties.

In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with CHSU, as well as any other form of electronic communication.

The same principles and guidelines found in the CHSU's policies and three basic beliefs apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of fellow employees or otherwise adversely affects students, customers, suppliers, people who work on behalf of CHSU or its legitimate business interests may result in disciplinary action up to and including termination. If you have questions or need further guidance, please contact the Office of Student Affairs for your College.

Be Aware: Carefully read these guidelines and CHSU's other policies, including but not limited to, anti- harassment and anti-discrimination policies to ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination of employment.

Be Respectful: Always be fair and courteous to fellow employees, students, customers, suppliers or others that you interact with. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers or supervisor rather than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage customers, students, employees or suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex, disability, religion or any other status protected by law or CHSU policy.

Be Honest and Accurate: Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about CHSU, a co-worker, a student, customers, suppliers, other people working on behalf of CHSU or CHSU's competitors.

Be Appropriate: Being appropriate when using social media means the following:

1. Maintain the confidentiality of CHSU's trade secrets and private or confidential information. Trades secrets may include information regarding the development of systems, processes, products, know- how and technology. Do not post internal reports, policies, procedures or other internal business- related confidential communications.
2. Respect financial disclosure laws. It is illegal to communicate or give a "tip" on inside information to others so that they may buy or sell stocks or securities. Such online conduct may also violate Federal insider trading laws.
3. Do not create a link from your blog, website or other social networking site to CHSU's website without identifying yourself.
4. Express only your personal opinions. Never represent yourself as a spokesperson for CHSU or its affiliates. If CHSU is a subject of the content you are creating, be clear and open about the fact that you are a student/employee and make it clear that your views do not represent those of CHSU, fellow employees, students, customers, suppliers or people working on behalf of CHSU. If you do publish a blog or post online related to the work you do or subjects associated with CHSU, make it clear that you are not speaking on behalf of CHSU. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of CHSU."
5. Dispensing of medical advice or expression of professional opinions on social media is prohibited. For dissemination of relevant and appropriate health information through the University's communication platforms, please submit all requests to the CHSU Marketing and Communications Department.
6. Interaction with patients on social media sites is prohibited.

Using Social Media in class or at Clinical sites is prohibited unless expressly a component of an assignment and authorized by the instructor and/or preceptor. During work hours or in clinical areas, the policy of that organization should be followed.

Using Social Media at Work: Refrain from using social media while on work time or on equipment provided by CHSU, unless it is work-related as authorized by your manager. Do not use your work email addresses to register on social networks, blogs or other online tools utilized for personal use.

Because the student to faculty and staff relationship has the potential to be power-based, faculty and staff are strongly discouraged from "friending" or otherwise connecting with current or prospective students on social media. Professional networking platforms (such as "LinkedIn") are permissible.

Retaliation Prohibited: CHSU prohibits taking negative action against any student or employee for reporting a possible deviation from this policy or for cooperating in an investigation. Any student or employee who retaliates against another employee for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination of employment and/or dismissal from the university.

Media Contacts: Students and employees should not speak to the media on the CHSU's behalf without prior approval of a supervisor. All media inquiries should be directed to the Vice President of Marketing and Communications.

Responsibility

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.

Restriction of Use

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.

Personally Owned Devices

Student using 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.

University Branding

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.

Reporting

If a student becomes aware of any security problem (such as any comprise of the confidentiality of any login or account information) or misuse of University Technology, he/she shall immediately report such information to the Office of Student Affairs of their respective college.

Consequences for Violation

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

Record of Activity

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.

Blocked or Restricted Access

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.

No Expectation of Privacy

Users 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.

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.

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. Students 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.