Computer and Network Acceptable Use Policy

The University's computing and network systems and services, "Chapman Information Resources" are a University-owned resource and business tool to be used only by authorized persons for educational purposes or to carry out the legitimate business of the University.

The Policy applies to all University students, faculty and staff, and all others using computer and communication technologies, including the University's network, whether personally or University owned, which access, transmit or store University or student information.

Below is a summary, as well as the full policy. The summary is not a substitute for the full policy and is only intended to help understand the policy. Users are required to comply with the entire policy.

Expand

Summary ⌄

Computer and Network Acceptable Use Policy ⌃

This policy covers the appropriate use of all Chapman Information Resources including computers, networks, application software and the information contained therein.

Authority:
University Review 2016

Applicability
Applies to all University students, faculty and staff, and all others using computer and communication technologies, including the University's network, whether personally or University owned, which access, transmit or store University or student information.

Policy Statement:
The University's computing and network systems and services, "Chapman Information Resources" are a University-owned resource and business tool to be used only by authorized persons for educational purposes and to carry out the legitimate business of the University.

Jump To:

1. Definitions

2. Policy

3. Acceptable Use

1. Definitions

As used in this policy:

a. "Chapman Information Resources" are all Chapman University-owned computer equipment, the operating systems and application software that reside on this equipment, and the networking hardware and software which connects this equipment. By extension, this policy applies to all Internet traffic that flows through such equipment.

b. "Personally owned resources" are Chapman Information Resources that are computers and devices under the control of University students, employees or agents and are not wholly owned by the University.

2. Policy

Free exchange of ideas is central to the mission of higher education. Chapman University respects and encourages the exchange and debate of ideas, including electronic interchanges. However, all communications conducted on University computers or networks should be business-like, courteous and civil. The protection of confidential, sensitive, and proprietary information is of critical importance to the University; therefore, it is essential that faculty, students and staff take steps to safeguard such information. The University does not condone messages of hate, bigotry, violence or intimidation directed at any individual or group, or harassment of any kind. Acts of harassment and threats will be thoroughly investigated by University, and may be subject to review by state and federal enforcement agencies.

All users of Chapman Information Resources agree to abide by the Chapman University Computer and Network Acceptable Use Policy. Use of Chapman Information Resources constitutes acceptance of the terms and conditions specified by these policies. The policy describes acceptable use of Chapman Information Resources, whether accessed through computers and devices owned by Chapman University, or through personally owned resources connected to the Chapman network, or remotely through outside equipment.

3. Acceptable use

As a condition of assessing Chapman Information Resources, you agree to comply with the following:

1. It is appropriate to use Chapman Information Resources for classroom and instructional activities, research related activities, correspondence and support, and administrative functions. Misuse includes but is not limited to violation of federal or state law, violation of University policy, unauthorized use of the system for commercial purposes, displaying sexually graphic images or text, abusive language, harassing behavior, unauthorized use of copy   materials, and excessive use for non-official or frivolous purposes.

2. University owned equipment and Chapman Information Resources services may not be used for illegal purposes. Users must abide by all software licenses, copyright and intellectual property policies and applicable federal and state laws. Plagiarism of electronic works is prohibited. The unauthorized use of copyrighted material is prohibited. This includes but is not limited to:

   - Reproduction of copyrighted materials, trademarks, or other protected material in any electronic form without express written permission from the material's owner;

   - Use, distribution or duplication of copyrighted software without appropriate licensing agreements, or use of software in a manner inconsistent with its license;

   - Use, distribution or reproduction, in any digital form, of copyrighted music, video, or other multimedia content without the express written permission of the material's rightful owner;

   - Copyright violations as they apply to all information available electronically.

3. Although Chapman University does not make a practice of monitoring e-mail The University reserves the right to retrieve the contents of University-owned computers or e-mail messages for legitimate reasons, such as to find lost messages, to comply with investigations of wrongful acts, to respond to subpoenas, or to recover from system failure.

4. Except as authorized, in writing or by e-mail, by the University, users are not to use Chapman Information Resources for compensated outside work, the benefit of organizations not related to the University (except in connection with scholarly, creative or community service activities), or commercial or personal advertising.

5. Unless otherwise protected by Federal labor laws, direct political campaigning and fundraising of any kind is considered an inappropriate use of Chapman Information Resources; however, general discussion and debate of political issues falling within the scope of intellectual activity is not discouraged.

6. The privilege of using Chapman Information Resources is provided by the University and is not transferable or extendable by members of the University community to people or groups outside the University.

7. Users are responsible for the use or misuse of their own accounts. Users are responsible for safeguarding their account passwords. A user should never use another person's account, or give his or her own password to another person for the purpose of gaining access to Chapman Information Resources. Account holders are responsible for all actions performed with their accounts.

8. The ability to read, alter or copy a file does not imply permission to read, alter, or copy that file.

9. It is unacceptable to try to bypass standard procedures, including attempting to discover another person's password, or to use an account for purposes for which it was not intended. Attempts to gain unauthorized access to machines via the network, to decrypt encrypted material, or to obtain privileges to which the user is not entitled are prohibited by public law. Attempts to circumvent data protection schemes, to discover security loopholes, or poss⌄ of software for such purposes by users are prohibited. Port scanning or other network vulnerability scanning to discover open services on computers inside or outside the Chapman network is prohibited except for use by the Network Operations staff of the Information

Systems & Technology Department (IS&T) who, with the knowledge and permission of the Chief Information Officer, may use this technique to monitor the Chapman network.

10. It is unacceptable to intentionally distribute a computer virus or engage in any procedure that interferes with the normal operation and delivery of services over the network.

11. Users of Chapman Information Resources assume the responsibility for backing up their own data and programs.

12. No person shall use or cause to be used any software on the University's computers that does not fall into one of the following categories:
    (a)   It is in the public domain.
    (b)   It is covered by an effective licensing agreement with the software author, authors, vendor or developer, whichever is applicable.
    (c)   It has been donated to the University and a written record of a bona-fide contribution exists.
    (d)   It has been purchased by the University and a record of a bona-fide purchase exists.
    (e)   It has been purchased by the user and a record of a bona-fide purchase exists and can be produced by the user upon demand.
    (f)   It is being reviewed or demonstrated by the users, pursuant to permission given by the owner, in order to reach a decision about possible future purchase or request for contribution or licensing.
    (g)   It has been written or developed by a Chapman University employee for the specific purpose of being used in the University's computer environment.

13. The Executive Vice-President and Chief Operating Officer of Chapman University is designated as the only individual who may sign license agreements for all software for Chapman University.

14. Copying of computer software may be done only in compliance with the published copyright and licensing agreements provided with the purchase of all software.

15. Use of peer-to-peer file sharing software through which files are made available to other users, are prohibited unless authorized by the IS&T Department.

16. Chapman Information Resources users who wish to create web sites on Chapman's web servers agree to abide by the guidelines in set by Strategic Marketing & Communication department.

17. All users of Chapman Information Resources must observe the policies of other networks that they may access.

18. Chapman Information Resources users may not conceal or misrepresent their identities when sending e-mail messages.

19. Chapman Information Resources users should keep in mind that many people use the Chapman Information Resources network for daily work. Behaviors that inhibit or have the potential to inhibit the ability of others to utilize shared computing resources are considered policy violations. Such behaviors include but are not limited to:
    (a)   Exceeding limits for resource usage (e.g. disk space, bandwidth, CPU time). Allowable

limits are determined by the IS&T Department.

(b)   Providing access to Chapman resources to individuals outside the university community.

20. The Chapman Information Resources system may not be used for playing computer games if such activity is detrimental to the use of Chapman Information Resources for academic, research or university business purposes in the judgment of the IS&T Department.

21. Regardless of available encryption methods or other security, users should understand even with the commitment to safeguard Chapman Information Resources, it is impossible to eliminate all risk of breach; therefore, every effort should be made to secure data that is considered highly sensitive, confidential or personal.

22. All wireless traffic is presumed to be insecure and susceptible to unauthorized examination. Due to this lack of privacy, users should not use the wireless network to access critical and essential applications or transmit sensitive material and information, social security numbers or credit card information. Individuals assume full responsibility and accountability for wireless network communications. Chapman University will take precaution to minimize this exposure and will proactively introduce new technologies, when available, to secure and safeguard network traffic.

23. Chapman maintains broad wireless coverage throughout the Orange Campus, Rinker Campus and Residential Complex. In order to provide the best overall performance and security for this wireless service, personal wireless routers are not allowed. Any wireless device that is found to interfere with the proper operation of Chapman's wireless network is prohibited. This can include some portable telephones that operate in the 2.4 GHz or 5 GHz frequency bands.

24. When connecting personally owned resources to Chapman Information Resources, the user of those computers must takes steps to make sure that the computers are free from security vulnerabilities and viruses. In particular, these computers must have operating systems that are supported by their manufacturers and must have antivirus software packages installed which are updated with the latest antivirus data files. Users must download and install the latest operating system and application software security patches. Security patches can be downloaded at no cost to the user.) The IS&T department reserves the right to specify procedures that must be followed when connecting personally owned resources to Chapman Information Resources.

25. Each user is ultimately responsible for his or her own computing and his or her own work using a computer. Users should take this responsibility seriously. For example, users should remember to make backup copies of their data, files, programs and tapes, particularly those created on desktop computers and those used on individually or departmentally operated systems. Furthermore, users with desktop computers or other computers that they operate themselves must remember that they may be acting as the system administrators for those computers and need to take that responsibility very seriously.

26. It is the user's responsibility to review, understand and comply with this policy. The University is responsible to assure that all users are made aware of the policy and have access to the   t recent version of it. Questions regarding the provisions and interpretations of this policy be directed to the Chief Information Officer or his/her designee.

4. Consequences of Misuse

The university reserves the right to restrict the use of its computing facilities and limit access to its networks when faced with evidence of violations of university policies or standards, contractual obligations, and federal, state or local laws. Violations of the law or policy may result in discipline and may be reported to the appropriate authorities outside the University.

Any actions which deter others from doing their work or which would be otherwise deemed malicious will result in the loss of access to the system and possible University disciplinary action and/or civil or criminal actions.

Misuse of Chapman Information Resources may result in:

- Loss of computing privileges and may require financial restitution to the University for losses incurred by the University.
- University disciplinary action and/or civil or criminal actions.
- The unauthorized use of Chapman Information Resources or the use of Chapman Information Resources for personal gain may constitute theft or other violations under California and Federal law and may be a prosecutable offense.
- Referral to the appropriate University officials for disposition in accordance with the applicable policy governing the individual's conduct and/or law enforcement authorities.

5.Reporting Policy Violations

If a person believes that a violation of this policy has occurred, he/she should contact the IS&T service desk or Information Security office.

Leaving Chapman University

Microsoft Teams Security Policies

Printing Policy

Privacy Policy

Privacy Practices

UG Student Worker Canvas Access

Contact Us

Maps & Directions

Emergency

ORANGE CAMPUS

One University Drive
Orange, CA 92866
(714) 997-6815

RINKER HEALTH SCIENCE CAMPUS

9401 Jeronimo Road
Irvine, CA 92618

GET STARTED

Visit Chapman

View Tuition and Aid

Apply Now

Employment

DISCOVER

Schools and Colleges

Programs at Chapman

Events at Chapman

Newsroom

Directory

SUPPORT

Report Concern or Incident

Accessibility Feedback

Website Feedback

Disability Services

Consumer Disclosures

Privacy Policy

Title IX