Copyright at Claremont School of Theology

Copyright Policy

It is the policy of Claremont School of Theology to uphold and comply with the U.S. Copyright Act. Copyright is a special protection, granted by law, for original works of authorship that exist in a fixed, tangible form, whether published or unpublished, including books, textbooks, journals, articles, songs, videos, games, software, and other creative content. The Copyright Act gives copyright owners specific exclusive rights (namely the rights to make copies, distribute the work, display or perform the work publicly and to create derivative works). Unauthorized copying or unauthorized distribution of copyrighted material is a violation of the U.S. Copyright Act. Claremont requires all faculty, students and staff to honor copyright and not copy or share protected materials in any way that would violate the law. Consistent with this law, Claremont policy prohibits the unauthorized copying or unauthorized distribution of copyrighted works, and prohibits the unauthorized distribution of copyrighted works through peer-to-peer file sharing. This unauthorized use may also violate civil or criminal law. Claremont's Acceptable Use Policy (AUP) extends this policy to Claremont's computing resources and states that all users of the School's network must not use the campus network to engage in any illegal downloading, emailing, or peer-to-peer file sharing of copyrighted works. Claremont is required by law to take steps to prevent illegal copying or distribution, and to respond appropriately to all complaints regarding copyright infringement.

There are certain allowable exceptions for U.S. academic institutions that permit a limited amount of copying without permission, if specific criteria are met. The five exceptions to the exclusive rights of copyright holders are the principle of fair use, the face-to-face teaching exception, the distance learning exception articulated in the TEACH Act, the first-sale doctrine, and the library and archives exception. For more information on these exceptions, see Fair Use of Copyrighted Materials, developed by the University of Texas.

Claremont students, faculty and staff must have permission from the copyright holder, or a determination that "fair use" applies, before files are copied, made available, or shared on networks.

- For the full text of the copyright law, and related laws, read U.S. Copyright Law.
- For a wealth of information about copyright, see the U.S Copyright Office.
- For a clear explanation of copyright law, take the Crash Course in Copyright, developed by the University of Texas.

Claremont School of Theology
Compliance with the Higher Education Opportunity Act (HEOA)
Peer-to-Peer File Sharing Requirements

The Higher Education Opportunity Act requires all U.S. colleges and universities to comply with its new regulations, which deal with issues surrounding the distribution of copyrighted materials, particularly through peer-to-peer file sharing. These new regulations require Claremont School of Theology to take four actions: an annual disclosure regarding unauthorized distribution, a plan to combat unauthorized distribution, a disclosure of alternatives to illegal downloading, and a review of the effectiveness of the plan to combat unauthorized distribution. What follows below is the action Claremont has taken to implement each of these requirements.

Annual Disclosure

Claremont is required to issue an annual disclosure to all students, informing students that the unauthorized distribution of copyrighted materials may subject students to civil and criminal penalties. Claremont is also required to disclose the steps it will take to detect and punish copyright infringement.

Annually, during the Fall Semester, the Chief Information Officer will distribute a communication to all students regarding Claremont's policies on copyright and peer-to-peer file sharing, the steps the School will take to enforce its policies, and the legal penalties for copyright infringement. This communication will also remind all students of our Acceptable Use Policy and the procedures Claremont will follow in responding to DMCA notices.

Plan to "Effectively Combat" the Unauthorized Distribution of Copyrighted Material by Users of the Claremont School of Theology Network

Claremont must certify to the Secretary of Education that it has implemented a plan to effectively combat the distribution of copyrighted materials through its network. Claremont's plan must included the following components:

I. Community Education and Information

Consistent with the value we place on our educational principles, we view education as the most significant measure we can take to combat illegal file sharing at Claremont. We use several mechanisms to inform and educate our community regarding copyright and related issues.

The Copyright at Claremont Web Page is maintained by the Office of the Chief Information Officer, and provides information concerning copyright law, and consumer information and disclosures that are required by the Higher Education Opportunity Act.

The Claremont Digital Millennium Copyright Act (DMCA) and Notification Procedures describe the procedures and disciplinary action that the School will use for handling cases of alleged copyright infringement, illegal downloads, and illegal peer-to-peer file sharing. Claremont School of Theology will respond firmly and appropriately to all instances of alleged copyright infringement on its network, as well as instances in which Claremont School of Theology students have allegedly engaged in illegal activity on the networks of the Claremont University Consortium and the Claremont Colleges.

Claremont's Acceptable Use Policy describes acceptable and unacceptable use of Claremont's computing resources and network.

New Student Orientation on Copyright and Peer-to-Peer File Sharing is a required tutorial for all new students and will be implemented at the beginning of the fall 2011 semester. Included in this tutorial are the techniques students may use for Disabling Peer-to-Peer File Sharing (developed by the University of Chicago).

New Student Orientation Letter on safe and legal computing will be included in the information packets for new students at the start of each academic term, beginning in summer 2011.

II. Technology-Based Deterrents

Claremont is planning a major upgrade to its technology infrastructure, and intends to implement bandwidth-shaping mechanisms.

Legal Alternatives to Unauthorized Downloading and Illegal File Sharing

Claremont is required to disclose legal alternatives to unauthorized downloading and illegal file sharing.

Educause maintains a comprehensive list of Legal Sources of Online Downloading, and the Association of American Publishers provides a list of Sources for Legally-Available Digital Versions of Textbooks and Other Written Works. Claremont encourages its community to make use of these resources.

Reviewing the Effectiveness of this Plan to Combat Unauthorized distribution of Copyrighted Materials.

Claremont will review the effectiveness of its *Plan to Combat the Unauthorized Distribution of Copyrighted Material by Users of the Claremont School of Theology Network* annually. This review will be managed by the Chief Information Officer, assisted by Information Technology Staff and the Institutional Research Council. Instances of alleged copyright infringement will be tabulated annually and longitudinally, and this data will be compared with that of peer institutions.

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.

Claremont's Digital Millennium Copyright Act (DMCA) Notification Procedures

DMCA (Digital Millennium Copyright Act) Notifications (sometimes called "Takedown Notices") are formal complaints delivered to the School, giving notice of an alleged copyright infringement on the network. This complaint will typically indicate the name of the file, the date and time this alleged infringement occurred, the specific IP address of the offending computer, and it will demand that the materials and/or access to the materials be removed from the computer. When a DMCA notice is received, Claremont will respond quickly to remove or disable access to the material for which an infringement has been claimed. Specifically, the School will:

For a first offense:

- Forward the DMCA Notification to the person who is responsible for the computer mentioned in the notice.
- Request that the user contact the Chief Information Officer within 5 days of receiving this notification.
- Ask if the user has downloaded or shared this copyrighted material without permission.

If the user acknowledges unauthorized downloading or sharing, we will:

- Request the user to remove the materials.
- Request that the user disable file sharing of all copyrighted materials on his or her computer.
- Require the user to read the Acceptable Use Policy and Claremont's information regarding copyright and peer-to-peer file sharing.
- Require the user to submit a written statement that confirms this infringement, acknowledges violation of the Acceptable Use Policy, and promises not to repeat this activity.
- Deny network access to this user for 5 days.
- Inform the claimant that the matter has been resolved.

If the user denies unauthorized downloading or sharing, we will:

- Require the user to submit a written statement denying this copyright infringement claim;
- Inform the claimant that this claim has been denied;
- Inform the user that under the DMCA the claimant may pursue a subpoena to obtain the users identity and may file a lawsuit against this user.

For a second or repeating offense:

- Forward the DMCA Notification to the person who is responsible for the computer mentioned in the notice.
- Request that the user contact the Chief Information Officer within 5 days of receiving this notification.
- Ask if the user has downloaded or shared this copyrighted material without permission.

If the user acknowledges unauthorized downloading or sharing, we will:

- Request the user to remove the materials for his or her computer.
- Request that the user disable file sharing of all copyrighted materials on his or her computer.
- Require the user to re-read the Acceptable Use Policy and Claremont's information regarding copyright and peer-to-peer file sharing.
- Require the user to submit a written statement that confirms this second alleged case of infringement, acknowledges violation of the Acceptable Use Policy, promises not to repeat this activity, and recognizes that any further violations will result in disciplinary action being taken against the user.
- Deny network access to the user for 5 days.
- Inform the Academic Dean and the Dean of Students of actions taken.
- Inform that claimant that the matter has been resolved.

Claremont's Technology Acceptable Use Policy

Purpose

In support of its mission to instill students with ethical integrity, religious intelligence and intercultural understanding, Claremont School of Theology provides access to its technological resources to its employees, students and other authorized users. These resources include electronic media and services, computers, email, telephones, voicemail, fax machines, computing and telecommunications networks, software, databases, intranet, Internet and the World Wide Web. The purpose of these resources is to strengthen the various research, teaching, learning, and administrative functions that fulfill the School's mission.

Claremont School of Theology encourages innovative use of technology in the pursuit of educational excellence, as well as effective and efficient use of technology throughout all academic and administrative departments. But all users must bear in mind that these electronic resources (including software, hardware, network equipment and capability) and all data stored in the School's facilities are the property of the institution, and that the use of these resources is a revocable privilege, and not a right of employment or matriculation. All use of these resources must be responsible and lawful, and in compliance with institutional policies.

One of the main characteristics of Claremont's computing systems is that they are shared resources. There are many computing activities that can occur on a network which interfere with, or undermine the work of others. Some of these activities may be illegal and malicious, while others may be merely accidental or uninformed. The following policy defines user responsibilities, acceptable use, unacceptable use and its consequences. It is applicable to all users of these systems: students, faculty, staff, and administrators of Claremont School of Theology and its affiliated centers; external users of public computers in the Library, Computer Lab, and Community Center; and users who connect personal laptops to the School's wired and wireless networks.

User Responsibilities

The use of technology at Claremont School of Theology is a privilege, and all users must act responsibly. Users must:

- Respect the rights of other users of the Claremont School of Theology's networks,
- Respect the integrity of these computer systems, and observe relevant laws,
- Become familiar with, and abide by, all applicable institutional policies, and

- Practice responsible computing (such as backing up data, protecting against the intrusion of computer viruses, safeguarding passwords and network security, and taking reasonable steps to minimize the influx of spam).

Acceptable Use

Acceptable use includes, but is not limited to:

- Electronic communication that is used for the academic and business purposes of the institution.
- The use of computing and networked resources for faculty and institutional research, classroom teaching, student learning, publishing, and accessing Library resources.
- The use of technology to help fulfill the business functions of the institution and its affiliated centers.
- Approved use of Claremont School of Theology Web site for public education, institutional promotion and fundraising, and to encourage research.
- Using online databases to retrieve relevant information for academic, administrative, or professional use.
- Because these computers, technology services, and telecommunication networks are primarily for the academic and research use of students and faculty, and for the administrative use of employees, limited, occasional, and incidental use for personal or non-business use is permitted. However, such use must be done in a manner that does not interfere with the user's employment, the proper functioning of equipment, or the proper functioning of a department or other institutional obligations, and in a manner that does not incur additional costs for the institution.

Unacceptable Use

Unacceptable use includes, but is not limited to:

1. Unacceptable Electronic Communication

- The use of electronic communications (such as email, messaging, chat rooms, electronic discussion groups, newsgroups, listservs, and social networking tools) to knowingly transmit messages or materials that are discriminatory or harassing, intimidating, derogatory, obscene, defamatory or threatening, libelous, slanderous, fraudulent, or that use vulgar or abusive language.
- Forging electronic messages, or transmitting disinformation.

- Transmitting unauthorized bulk mail, mass email, junk email, sending or forwarding chain email, sending excessive messages, or any transmissions that consume substantial computing resources or bandwidth.
- Unauthorized interrupting or monitoring of electronic communications.
- Communicating in ways that imply institutional endorsement, unless authorized to do so.
- Any use of Claremont School of Theology computers, networks, or Web sites for personal advertisements, solicitations, promotions, personal gain, business ventures, or private profit.

2. Unacceptable Computer Use that Undermines System Integrity

- Modifying, damaging, removing, or stealing computing resources, equipment, software, cables, networks, or furniture that is owned by the Claremont School of Theology. (Calif. Penal Code § 502.)
- Any attempt to intercept, monitor, tamper with, read, copy, alter, or delete a file or program belonging to another person or office, without authorization of the owner.
- Any connectivity to a network that poses safety or electrical hazards.
- Knowingly performing any activity that interferes with the normal operations of any computers, components or networks.
- Using services or computer systems or the Internet in such a way as to cause network congestion.
- Deliberately wasting computing resources.
- Excessive printing.
- Developing, installing, transmitting, delivering or running any program that is intended to cause damage to a computer system, or place a heavy load on a computer or network (including computer viruses, Trojan horses, worms, and other malware).
- Installing unauthorized software or equipment on School-owned computers.

3. Unacceptable Access

- Using a computer account that is assigned to someone else.
- Disclosing one's assigned password to another person, without authorization.
- Obtaining a password for an account without authorization.
- Using the Claremont School of Theology network to gain unauthorized access to any campus system, program, database, or file.

- Any attempt to circumvent security and data protection schemes, or to discover security loopholes, or decrypt secure data
- Masking the identity of an account, a computer, or a transaction.
- Unauthorized breaching, probing, testing, or monitoring computer or network security.
- Use of campus computing resources by any user younger than 18 years of age.

4. Use that Disrupts or Disrespects Others

- Any use that does not respect the rights and needs of others.
- Violating the privacy of other users
- Disseminating confidential personnel or student information without authorization, or distributing proprietary financial information.
- Any activity that creates a hostile study or working environment, including sexual harassment.

5. Violations of Copyrights, Contractual Agreements, and Licenses

- Distributing or making copies of software, unless permitted by copyright law or software license agreements.
- Distributing or making copies of documents, works of art or other intellectual property, unless permitted by copyright law.
- Using peer-to-peer file sharing protocols or programs to download or distribute unauthorized copies of copyrighted materials.
- Having more simultaneous users (e.g., in a department) than permitted by software license agreements.
- Using copyrighted material without proper attribution.
- Violating terms of software license agreements, or copyright laws.

Additional Use Policies

Users must also comply with additional applicable computer and network use policies, such as Computer Lab Policy, departmental policies, etc.

Warnings

- Though Claremont School of Theology does not routinely monitor and evaluate every electronic transaction, document, file, or communication, it reserves the right to monitor access and use of its computing and

networking resources to insure the security and optimal performance of its network, to enforce its policies, to investigate possible violations of its policies, or to comply with civil authority. Claremont School of Theology's IT staff have the right to examine systems and files that might be damaged or corrupt, as well as files associated with suspended computer accounts.

- The School reserves the right to limit or curtail access and computing privileges when state or federal laws or institutional policies are being violated.
- Though the School may authorize confidential passwords and secured access to resources, users of the Claremont School of Theology network and systems have no expectation or guarantee of privacy in any communication sent or received over the Claremont School of Theology network, or over the Internet.
- The computing and telecommunication systems log many user transactions: such as telephone numbers dialed, call length, Internet sites visited. Claremont School of Theology reserves the right to gather and monitor this data for cost analysis, resource allocation, optimum technical management of information resources, troubleshooting computer problems or compromises in network security, detecting patterns of use that might indicate unacceptable use of the system, and investigating allegations of unacceptable use.
- Claremont School of Theology is not responsible for lost or corrupted personal files or data, or for any financial loss as a result of personal information that a user discloses across a network (such as a credit card number).
- Claremont School of Theology does not assume any responsibility for the content a user may discover on the Internet, newsgroups, or other online services. Some of this content may be objectionable, offensive, inaccurate, or dated. Claremont School of Theology also does not endorse any content that may be accessible through its computer networks and services.

Consequences of Unacceptable Use

Consequences of unacceptable use may include any or all of the following: informal email or conversation when infractions appear to be accidental in nature, verbal warnings, suspension or revocation of access privileges to technological resources (including passwords and email accounts), the suspension or revocation of Library privileges, formal disciplinary action as authorized by institutional policies (up to, and including, suspension or termination from employment, or, in the case of students, dismissal), and, in cases when law has been allegedly violated, referral for criminal or civil prosecution.