TECHNOLOGY ACCEPTABLE USE POLICY

Purpose

In support of its mission to instill students with ethical integrity, religious intelligence and intercultural understanding, Claremont 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 Web. The purpose of these resources is to strengthen the various research, teaching, learning, and administrative functions that fulfill the School’s mission.

Claremont 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 and its affiliated centers; and users who connect personal laptops to the School’s wired and wireless networks.

User Responsibilities

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

- Respect the rights of other users of Claremont’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’s web sites 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’s 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 Claremont. (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’s networks 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 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’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 Claremont’s network and systems have no expectation or guarantee of privacy in any communication sent or received over the Claremont 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 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 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 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 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.

Reproduction or distribution of copyrighted works, including images, text, and software, without permission of the owner is a violation of U.S. Copyright Law, and is subject to civil damages and criminal penalties.