Claremont School of Theology
Student Computing Policy and Technical Recommendations

General Information

Claremont School of Theology abides by all Federal, State, and local laws that apply to the electronic environment provided for the use of its students and employees. Claremont School of Theology is responsible for all traffic carried on its networks and reserves the right to monitor and to restrict network traffic considered to be detrimental to the networks themselves or to the community.

Campus computer networks and resources are maintained for the common, shared use of students and employees. Because network use is too far-ranging to completely list prohibited uses and behaviors, all users are to exercise good judgment regarding network use and to be considerate of other users. First-time incidents will be considered accidental and an opportunity for educating the user about network use. Repeat offenses will be referred to appropriate campus bodies for disciplinary action.

Policies

1. Student-owned computers are solely the student's responsibility.
    a. Campus information technology employees are not authorized to repair or to maintain student-owned computers. This applies to both hardware and software.
    b. Assistance may be rendered to establish connections to campus-owned computer networks.
2. Electronic communications are to be used carefully and responsibly, including but not limited to email, chat, and social networks. Prohibited behaviors include:
    a. Threatening communications, including harassment and bullying
    b. Forgery, identity theft, and misrepresentation
    c. Bulk transmission of junk mail or content not of general interest to the community
    d. Communications that are hostile and/or insulting ("flaming")
3. Behaviors that adversely affect network performance are prohibited, including:
    a. Excessive consumption of network resources
    b. Intentional attempts to compromise security (hacking) of either campus computers or any outside site
    c. Unauthorized networks
    d. Providing network access to unauthorized individuals
    e. User account sharing
    f. Individual commercial activity
4. Copyrights and other intellectual property are to be respected.
    a. The proper use of copyrighted and other protected intellectual property is a serious matter, covered under federal laws. Violations can incur both civil and criminal penalties.
    b. All students must receive training on the appropriate uses of intellectual property and sign a statement acknowledging that they have received such training and are aware of their responsibilities in this regard.

Recommendations

To work well and to succeed, students are advised to acquire a computer no more than two years old. Such a computer can likely last three years (or more) with normal maintenance. Any hardware or software products mentioned are merely for your information and are not endorsed by the school.

Laptop and Desktop Computers

The minimum recommendations that follow are for laptop computers, but the standards apply equally to desktop computers. Students are expected to be familiar with the operation and the maintenance of their electronic devices.

Hardware

- A two-year old or newer laptop running the originally-equipped operating system (Windows, Mac OS, Linux, etc.) or upgraded to a newer operating system, with all necessary security updates and patches installed
- 802.11g wireless network card (typically built-in on two-year old laptops) for access to the campus wireless networks
- Functional video and sound

Software

- Popular anti-virus, anti-malware, spyware software suite with a current subscription (Norton, McAfee, Kaspersky, etc.). Free anti-virus options include AVG, Avira, and Avast, available at download.com. *Do not run more than one anti-virus suite as these programs will conflict with each other*.
- Word processor able to produce and to edit .doc and .docx files. Free options include GoogleDocs, available at docs.cst.edu or through your own Google account, and openoffice.org
- Web browser
- Adobe Acrobat Reader (free at www.adobe.com)

The above, minimum configuration will help to create a satisfactory experience. Most laptops two-years old or newer will meet the hardware requirements. A newer laptop has a greater chance of meeting a student's needs for the duration of his/her studies.

Tablet Computers

As of fall 2012, tablet computers are not recommended as a viable laptop computer or desktop computer replacement. Tablets do not perform the full-range of computer functions necessary to meet academic demands.

On-Campus

Laptop computers and most tablet and mobile devices will connect to the campus network.

Power outlets are somewhat scarce in the classrooms. Students may wish to bring a small power strip to share electricity with their colleagues.

The campus wireless network is password-protected. Students will be informed in advance of password changes.

Do not leave your laptop, or other personal property unattended.

Home Network

At home, a digital subscriber line (DSL) is the recommended minimum for a smooth experience with video and audio files delivered via the internet. Higher speed connections will improve the experience. Access to campus services are primarily via web browser.

Computer Hygiene

Students are reminded that it is far easier to prevent malicious attacks on their computers than it is to repair them when they are infected. A quality computer protection suite is a small expense when weighed against the potential loss of data, both personal and academic. Be suspicious of any software downloads from unknown or untrusted sources. Often, infections are piggybacking on free downloads, especially executable (.exe) and compressed (.zip, .rar) files and may not be identified by even the most current anti-virus software. Virus infected computers may be prohibited from network access to prevent the spread of infection.

Students are also reminded to periodically back-up their data to removable media or to off-site services. This will guard against the loss of data due to system failure or to system loss or theft.