CBTS Policy on Ethical Use of Seminary Owned Technology Resources

All Central Baptist Theological Seminary (CBTS) faculty, administrators, staff, and students, by virtue of their use of CBTS information technology resources, accept the responsibility of using these resources only for appropriate seminary activities.

This policy covers all information technology resources that provide the CBTS community with computing, networking, telephony, and television/video resources.

Information technology resources provide the CBTS community and guests with access to local, national, and international information as well as the ability to communicate with other users worldwide. Information technology resources should be used in an acceptable and ethical manner. For the benefit of the community, users must assume responsibility in the use of information technology resources. Use of information technology resources is governed by the United States Code, the laws of the state in which the technology is being used, and CBTS policies.

Authorized Access

Members of the CBTS community are authorized to use information technology resources provided by the Seminary. The CBTS Library provides public computers with access to the Internet. Library public computers are primarily intended for research, and research usage takes priority over other possible legitimate use of those computers.

Acceptable Uses

Information technology resources can be used for activities that support the mission of the seminary, which includes:

- Learning
- Teaching
- Research
- Seminary business

Appropriate personal communications are permitted as long as they do not detract from, interrupt, or interfere with the classroom or work performance of the student or employee of CBTS.

CBTS Data Network Connection Policy

Devices which extend the network such as but not limited to hubs, switches, bridges, routers and access points or computers functioning as such may not be connected to the CBTS data network without permission from the Office of the Executive Vice President. Such devices are connected by service personnel determined by that office. Users (students, faculty and staff) may connect computers and printers to the CBTS network.

Legal Use Guidelines

- Information technology resources may not be used for any illegal or criminal purposes.
- Software, images, music or other intellectual property may only be used in compliance with the U.S. Copyright Act and any other CBTS intellectual properties policies.
- Transmitting images, sounds, or messages to others which might reasonably be considered harassing, malicious and/or cyber bullying is not permissible.
- Use of CBTS technological resources for intentionally viewing or transmitting material that might reasonably be considered pornographic (as distinct from artistic materials) is prohibited with the exception of an approved research project. In such cases for your protection written permission should be obtained from either the professor of the course for which the project is being undertaken (if a student) or the Dean (in the case of faculty).
- Using CBTS information technology resources to attempt to break into, gain root access, probe, disrupt, or obstruct any system is not permissible. Installation of invasive software or testing security flaws without authorization on any system is not permissible.

Responsible and Ethical Use Guidelines

- Respect the intended use of all information technology resources for learning, teaching, research, and university business purposes.
- Respect other users by not sending unwanted email messages, personal advertising, maligning address information, flooding the system, sending frivolous messages, forging subscriptions, or tampering with accounts, files, or data that are not owned by your account.
- Use only the user credentials assigned to you; use it for the purposes which it was intended, and do not share it with others.
- Be sensitive to the public nature of shared resources, i.e. labs, modem pool, disk space, printers, bandwidth, etc.

- Observe all legal requirements specified in any software licenses, contracts, and copyright.
- When using networks outside of CBTS (such as the Internet) to conduct seminary business or study, comply with the acceptable use polices and contracts of those systems.

Reporting Misuse of Information Technology Resources

Complaints regarding misuse of information technology resources should be reported to the Office of the Executive Vice President in the case of administration or staff and to the Dean in the case of faculty or students.

Information Technology Services' Responsibilities

The Office of the Executive Vice President is responsible for insuring that the Seminary's computing, networking, television/video and telephony resources are properly used and protected by maintaining the integrity, security, and privacy of the resources and of users' electronic files, mail, records, and activities. The Assistant to the Dean administers many of these matters relative to educational, faculty and student needs.

While the seminary does not generally monitor or limit content of information transmitted on the network, it reserves the right to access and review all information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or records search, as may be necessary. Users should not expect that their use of information technology services, (sites they visit, email, IM, files, network traffic, etc.) while using seminary resources will be private, except those related to faculty, employee, and student records that are protected under federal or state privacy laws. Those files are secured and only may be viewed by persons authorized to access them. Such data is secured in servers that meet federal privacy standards, are identified as secured sites, and are password protected.

Supervision

CBTS courses offered online are subject to supervision by the Dean's Office, the Director of Online Course Design, and the Assistant to the Dean only for purposes of compliance, technical repair/maintenance, resolution of student operational problems, and quality. Such supervision does not include accessing any exchange of information between professor and student, among students in the course, discussion forums, or any other communications that might contain confidential information except as necessary to resolve technical problems experienced by the professor and/or a student in the class and for unavoidable technical repairs and/or maintenance.

Whenever access to sensitive areas of an online class is necessary, a log will be kept of the access including: (1) the nature of and reasons for the access, (2) the date, and (3) the time. This log will be maintained by the Assistant to the Dean. In addition, the authorized person accessing the protected information will be subject to CBTS's codes of confidentiality and must guard any such information as confidential. Any invasion of student confidentiality through unauthorized access to student academic files, financial records, course work, or other protected information by a professor, employee, student, or other person is expressly prohibited and is subject to legal penalties and/or disciplinary action by CBTS including expulsion (if a student) or loss of job (if a faculty member or employee).

Access to the appropriate information and/or files by a professor or administrator for purposes of legitimate student advising, course work, and academic supervision does not constitute unauthorized access. In all cases, confidential information is password protected and access is granted only to persons authorized to share that information. Other employees are made aware of the confidential information they are permitted to access and with whom they are allowed to share the information. Should any faculty member, staff person, or other employee have questions regarding appropriate and inappropriate access to student information, consult the Dean's Office.

Investigations

Security measures are in place to assist with investigations of illegal and criminal activities or policy violations. Investigations performed by the Office of the Executive Vice President and the Office of the Dean are conducted as appropriate and necessary and within the guidelines of legal restrictions and regulations.

If suspicion of misuse of information technology resources is found, the following steps will be taken to protect information technology resources and the user community:

- Computing, networking, and telephony accounts will be immediately suspended pending the outcome of any investigation.
- Files, data, usage logs, etc. will be inspected for evidence.
- The violation will be reported to the appropriate authorities:
    - CBTS policy violations will be reported to the Dean's Office, the appropriate instructors, the appropriate site coordinator, a direct supervisor, or responsible administrator.
    - Legal violations will be reported to the appropriate law enforcement authorities.

Violations of this policy could result in revocation of access to information technology resources as well as seminary disciplinary and/or legal action.

Violators are subject to any and all of the following:

- Loss of information technology resources access
- Seminary disciplinary actions (as prescribed in the CBTS Catalog, Employee Handbook, Student Handbooks, or CBTS Faculty Guidelines and Expectations)
- Civil proceedings
- Criminal prosecution