

Texas College
Appropriate Use Policy
Version 1.0

This document sets forth the privileges of and restrictions on students, faculty, staff, and other users with respect to the computing and telecommunications systems located at Texas College. This includes desktop systems, hand-held computers, lab facilities, centralized servers, classroom technology, the campus network, dial-in services, etc.. This document attempts to define and give examples of various sorts of activities which are detrimental to the welfare of the overall community and which are therefore prohibited. It also describes the process by which violators are identified, investigated, and disciplined. It should be noted that some activities, which are legal, are in violation of this Policy and are prohibited with respect to College computing and network systems.

PLEDGE TO Faculty, Staff, and Students

Texas College is committed to maintaining its leadership position in the use of computer and communication technology to facilitate learning. The College promises to provide, as rapidly and as economically as is feasible, the following:

- * students, access to their information anywhere on campus.
- * faculty, the resources necessary to enhance teaching, learning and research.
- * staff, the tools necessary for a responsive service environment.

The College will normally respect privacy and attempt to safeguard information but cannot guarantee these privileges absolutely: the college can examine, at any time, anything that is stored on or transmitted by College-owned equipment.

PROVISIONS

You are entitled only to one person's fair share of the College resources unless written permission to the contrary has been granted by the appropriate Executive Officer and/or Committee. The examples given below are examples of prohibited activities, not lists of everything that is a violation:

YOU MAY NOT steal, forge, lie or cheat with; snoop on; tamper with; misuse, damage, harass with; threaten with; hoard or monopolize; interfere with; violate the confidentiality of; masquerade with; or destroy any information, resource, equipment or software. This includes using your personal computer for these activities against other users or against their information resources.

Examples: You must not access the account of another; you must not generate activities, which consume more than your share of either system time or network bandwidth (including chain letters); you must not fraudulently log into any computer, etc.. You must not upload, post, or transmit content that harassing, threatening, libelous, invasive of another's privacy, hateful, or racially ethnically or otherwise objectionable. You must not forge e-mail headers or manipulate other identifiers in order to disguise the origin of any system or network activity.

YOU MAY NOT possess any software, resource, or equipment whose purpose is to effect one of the violations listed in the first Provision.

Example: You must not have in your account on any College-owned system or on your personal computer programs which attempt to determine the passwords of others or obtain privileges on any computer to which you are not entitled. **YOU MAY NOT** attempt to violate the first Provision. Any such attempt will be considered to be the same as a violation.

Example: If you attempt to obtain system privileges to which you are not entitled, you are as guilty as if you had succeeded. **YOU MAY NOT** possess, willingly receive, or distribute obscene material. **(TURN OVER AND READ BACK)**

Examples: Child pornography and other forms of pornography are absolutely against the law. It is a violation of Federal law to transmit this material across state lines, even electronically, and certain obscene materials are in violation of the **Texas Code and Law**. **References:** <http://www.capitol.state.tx.us/statutes/edtoc.html>

YOU MAY NOT violate the Information Technology Appropriate Use Policy off-campus anywhere in the world using College resources.

Examples: An attempt to gain unauthorized entry to any computer off the College campus is as if you attempted to gain access to a computer here. **YOU MAY NOT** copy, install or use any equipment, service, information, data, image, recording, or other work in violation of applicable copyrights or license agreements.

Example: If you use material created by or belonging to others, you must have their permission to do so.

YOU MAY NOT use any College facility for non-College commercial business or advertising, including unsolicited commercial e-mail without written permission from the Administration and/or Executive Staff. This includes partisan political activities.

Examples: You may not use the statistics software on the academic shared systems to do work for off-campus entities for which you are paid. The sending of unsolicited bulk e-mail (spamming) is not allowed. **YOU MUST** connect all equipment and install all software in a manner that meets the technical, security, and fair use standards set by Information Technology.

Examples: All IP addresses and domain names are owned and assigned by the College. World Wide Web, ftp, and other network services that interfere with fair network use by others may be restricted by the Office of Information Technology. You must follow proper use guidelines when using classroom technology, e.g., powering down projectors according to vendor specifications.

YOU MUST TAKE FULL RESPONSIBILITY FOR WHAT YOU PUBLISH, TRANSMIT, OR POSSESS.

COLLEGE-OWNED computer and network resources exist to advance the mission of the College. The College will manage these resources accordingly.

Examples: The College reserves the right to send official notices to all student/faculty/staff e-mail accounts. Campus webmasters should use discretion when linking to non-College websites. You may not install software on college-owned computers that interferes with day-to-day work or hinders the professional operation of college computers or networks.

PENALTIES

If you are suspected of violating this Policy, the College can impound any equipment, device, software, documents, or data that is involved. The College will obtain appropriate authorization before impounding anything.

If you have violated the Policy, you will incur the same types of disciplinary measures as violations of other College policies. Violation of state or federal free/statutes may lead to criminal or civil prosecution.

Students: Campus disciplinary measures may include, but are not limited to, failure in a class, permanent or temporary loss of information technology privileges, suspension or expulsion from the College, and restitution of expenses as well as charges for damages.

Faculty and Staff: Campus disciplinary measures may include, but are not limited to, reassignment of duties, transfer, censure, suspension, termination, and restitution of expenses as well as charges for damages.

Off-campus users: The College may revoke the privileges of users who are found to be in violation and may report any serious violation to the users home campus authorities and to appropriate law enforcement officials.