

## Texas County Technical College/Bolivar Technical College

### COMPUTER USAGE POLICY

#### **Purpose:**

Texas County Technical College (TCTC)/Bolivar Technical College (BTC) herein referred to as “College” provides access to computers and the Internet to assist students complete their training and to become well-informed citizens. The use of campus computers, networks, and other technical resources is a privilege and access can be revoked at any time for usage in contravention of this policy. By using or accessing the college’s technical resources, all individuals agree to comply with the security policy and the campus code of conduct along with all federal, state, and local laws. Use of the campus computers, networks, and other technical resources without authorization is prohibited.

The purpose of the college’s technical resources is to support education, research projects, and administrative services of the campus. All other uses of the college’s technical resources are secondary. Any type of activity that will prevent the technical resources of the campus from meeting their primary purpose may be terminated without notice.

All individuals granted Internet access with the college facilities will be provided with a written copy of this policy. All Internet users must sign the following statement:

I have received a written copy of the college Internet usage policy. I fully understand the terms of this policy and agree to abide by them. I realize that the school’s security software may record for management use the Internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file. I acknowledge that any message I send or receive will be recorded and stored in an archive file for management use. I know that any violation of this policy could lead to dismissal or even criminal prosecution. I agree to indemnify and hold the college harmless in any civil action brought under Federal or State law as a result of my violation of this policy.

#### **Policies:**

##### **Copyright and License:**

1. Software may not be copied without the owner’s permission, unless permitted by the copyright.
2. Acquiring a copy of someone else’s work in any form with or without the owner’s permission and presenting it as your own work is an act of plagiarism, which is forbidden. Individuals who provide their own work to others knowing they intend to present it as original work is strictly prohibited.
3. The use of the college resources will not be used to violate copyright or patent laws.
4. Individuals who access campus networking resources using their personal computer systems will not use those resources to acquire or distribute copyrighted works.

### **Security and Protection of Information:**

1. The college resources are protected by firewalls, proxies, Internet address screening programs, and other security systems to assure the safety and security of the school's networks. Any person who attempts to disable, defeat, or circumvent any school security facility will be subject to immediate dismissal.
2. Files containing confidential college information, data, trade secrets, and any other material covered by existing secrecy policies and procedures that are transferred in any way across the internet must be encrypted.
3. Individuals who use their own personal modems to create independent data connections sidestep the network security mechanisms. An attacker could use these connections to compromise the college network. Any computer used for independent dial-up or leased-line connections to any outside computer or network must be physically isolated from the college internal network.
4. Only those Internet services and functions with documented business purposes for the college will be enabled at the Internet firewall.
5. User ID's and passwords help maintain individual accountability for Internet resource usage. Any person who obtains a password or ID for an Internet resource must keep that password confidential.
6. Chat rooms and newsgroups are public forums, and individuals must refrain from revealing confidential college information, data, trade secrets, and any other material covered by existing secrecy policies and procedures. Persons releasing protected information through a newsgroup or chat room whether or not the release is inadvertent—will be subject to penalties, including dismissal from the college.

### **Social Networking:**

Texas County Technical College/Bolivar Technical College will maintain an official presence on social networking sites to support the college in accomplishing its mission and achieving its goal and objectives. The college encourages feedback and comments from fans, including prospective students, current students, alumni, faculty, staff and members of the community.

The college remains committed to maintaining these sites as a safe and family-friendly forum for sharing information. In maintaining a positive environment to site visitors, the college maintains the right to remove any comments or wall postings from official college-sponsored pages that are inappropriate, inflammatory or damaging to Texas County Technical College/Bolivar Technical College or any individual.

The college is responsible for posting materials to the college's main social networking sites. Instructors, program departments, and student organizations may also maintain other social networking pages for their specific needs and areas. If so, these should be approved by the campus director and approved prior to posting any material. The procedure for establishing social media

sites, general computer and social networking guidelines, and disclaimers are available on the college's main webpage and are provided to each student.

**Usage:**

1. The technical resources of the campus are shared resources and all individuals are expected to limit their use to a reasonable level and to limit their use to those activities that are consistent with this policy. The college reserves the right to deny or restrict an individual's access to these resources if the college determines that he or she has exceeded a reasonable level of use or has violated the provisions of this policy.
2. The use of the college technical resources to attack other resources or individuals to execute denial of service attacks against other networks, or to hack other networks is forbidden. Individuals will not use campus resources to spread viruses, worms, Trojan horse programs, trap-door programs, spam, chain e-mails, or hoaxes to other individuals. Performing these activities will be grounds to have all access terminated.
3. The display of any kind of sexually explicit image or document on any college system is a violation of policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited, or recorded using the college network or computing resources.
4. Any software or files downloaded via the Internet into the company network become the property of the college. Any such files or software may be used only in compliance with their licenses or copyrights.
5. No person may use the college facilities knowingly to download or distribute pirated software or data.
6. Each person using the college facilities shall identify himself or herself honestly, accurately, and completely (including one's affiliation with and function at the college).
7. Only those persons or officials who are authorized to speak to the media, to analysts, or in public gatherings on behalf of the college may speak or write in the name of the college on Internet resources. Other persons may participate in newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Unauthorized persons must refrain from endorsement or appearance of endorsement by the college of any commercial product or service not sold or serviced by the college, its subsidiaries, or its affiliates. Only those school officials who are authorized to speak to the media, to analysts, or in public gatherings on behalf of the college may grant such authority to participants.

**Technical:**

1. The college has software and systems in place to monitor and record all Internet usage. Our security systems are capable of recording each user's Internet site visit, chat room, newsgroup, e-mail message, and file transfer. No person should have any expectation of privacy as to his or her Internet usage.
2. The college reserves the right to inspect any and all files stored in private areas of its network in order to assure compliance with this policy.
3. The college retains the copyright to any material properly belonging to the college and posted to any forum, newsgroup, chat, or World Wide Web page.
4. To avoid affecting network traffic, persons should schedule communications-intensive operations, such as large file transfers, video or audio streams or downloads, and mass e-mailings to off peak times, if at all possible.
5. Any file that is downloaded must be scanned for viruses before it is run or accessed.