I. PURPOSE

This policy provides guidelines to protect the College, its computing resources and employees from liability, harassment and business interruptions due to inappropriate computer usage.

II. SCOPE

This document applies to all persons, using property owned or operated by CTCD, who have been granted use of Central Texas College’s computing resources for use at work, home or while traveling. Users include, but are not limited to, students, faculty, staff, vendors and guests of the College.

III. USE AGREEMENT

Computing resources are to be used only for the College-related activities for which they are assigned. These resources include all computer files, e-mail messages, Internet usage, voice mail messages and business telephone conversations on CTCD equipment. CTCD reserves the right to inspect any equipment and resources for prohibited files and downloads at anytime and for any reason. The College reserves the right to limit, restrict or extend computing privileges and access to its computing resources. Administrative units within the College may define additional procedures and conditions for use of computing resources under their control as long as they are consistent with this policy statement.

IV. USER RESPONSIBILITIES

All users of computing, networking, and other Information Technology (IT) resources of the College are required to:

A. be ethical and respectful of the rights of others and of the diversity of the College community;
B. protect the confidentiality and integrity of institutional data;
C. protect the integrity of passwords (computer accounts and passwords are for use only by individual users and should not be shared);
D. ensure computers are logged off when leaving their desk;
E. check regularly for operating system and browser software updates and security patches;
F. scan their computer for known viruses and other malicious programs that may be present;
G. backup files and folders regularly; and,
H. use resources responsibly and refrain from acts that waste resources or prevent others from using those resources.
I. abide by local, state, and federal laws.

V. INAPPROPRIATE USES

A. Using Emoticons/Wallpaper/Screensavers/Marquee Screensavers. The use of emoticons, wallpaper, marquee screensavers, and third party screensavers does not present a professional image. Their use can result in a loss of productivity, be offensive to some, and interfere with the normal functioning of other programs on your computer. Wallpaper and screensavers are limited to those included with the Microsoft Windows® operating system.

B. Sending personal e-mail. Personal e-mails are to be limited and will be closely monitored for abuse. Distributing joke e-mails, keeping in touch with friends, online dating, and sending resumes to prospective employers are examples of personal e-mail. E-mail accounts shall be used for the purpose for which they were created: College business communications. All violations will be reported. Employees that spend an excessive amount of time sending/receiving personal e-mail will be disciplined accordingly.

C. Storing personal data on College computers. This is an unauthorized use of the College’s computing resources. An example would be storing your resume in a Word folder, or using the address book feature of Outlook to store contact information for personal acquaintances.

D. Generating SPAM. Any e-mail, which is not official business, could be considered Spam if sent to everyone on the Outlook directory. Over time, the accumulation of these unsolicited e-mail messages will slowly degrade the performance of the e-mail system and generate unnecessary traffic on the network. It is preferable to use CTCD website links to communicate general information rather than to create mass, campus or district-wide e-mail messages.

E. Web surfing. Web surfing, including online shopping, and dating, consumes inordinate amounts of Internet bandwidth and causes business-processing bottlenecks.

F. Sending chain letters. These actions waste bandwidth, congest the e-mail system, and spread misinformation.

G. Running two or more concurrent sessions (connection between user and server). Multi-user computers do not have unlimited resources. If a user logs into a multi-user system such as Colleague two or more times (two or more concurrent sessions), he/she may prevent other users from having access to that computing resource.
H. **Listening to Internet radio.** Listening to Internet radio and other forms of non-work related streaming media consumes network bandwidth, thus taking resources from essential business processes.

I. **Using public IM tools or chat rooms (chatting).** Instant messaging may only be used when authorized by the employee’s supervisor and the IT Division. Use of instant messaging applications can seem easier and more convenient to use than the telephone or e-mail, yet they pose many risks to the College. Use of IM tools and chat rooms can affect employee productivity, waste network bandwidth, and pose a possible legal risk to the College. System security is also threatened as hackers can introduce viruses and worms into networks through files that are transmitted through IM tools and chat rooms. Hackers posing as legitimate business contacts can steal confidential information.

J. **Downloading/installing unauthorized applications.** Downloading or installing shareware, free screensavers, or games pose risks to user privacy and network security. These software applications can contain spyware that collect information about the user and send it to information collection services who will sell that information to third parties.

K. **Unauthorized use of confidential data.** When a user obtains access to data on a system, he or she must safeguard that information by not sharing it with third parties. Failure to do so poses a significant legal risk to the College and the user.

L. **Downloading MP3 music or movies to DVD.** Peer-to-peer (P2P) file-sharing programs such as Bit Torrent are used to illegally trade copyrighted music, movies, software, and games. Illegally copying or downloading copyrighted music, software, or movies (software piracy) is prohibited. P2P applications can leave a breach in an otherwise secure network, degrade network performance, provide unauthorized users access to your hard drive and the network, and can be an entry point into the network for malicious software. Many of the P2P programs contain spyware, allowing third parties to secretly gather information about users.

M. **Playing computer games.** Games adversely affect productivity. A number of gaming applications use excessive amounts of bandwidth, thus directing resources away from business critical tasks.

N. **Maintaining confidential data on desktops.** Unattended personal computers face exposure to theft and unauthorized access. Users shall always logoff of their PCs when they are away from their desks. Laptop shall not be left unattended and unsecured. Users must follow password guidelines, and install the latest software security updates. Laptops should have recovery software installed in the event of theft. Any PC with sensitive data and information should be safeguarded to reduce the possibility of theft and the resultant legal risks to the College.
O. **Destroying equipment, information, or data.** The confidentiality, integrity, and availability of computing resources can be compromised by the malicious or accidental damage of equipment, information, or data. Spilling coffee on a keyboard, dropping a laptop on the floor, and/or deleting files and data can result in resource and financial loss to the College. Reasonable precautions shall be taken with respect to the operation, handling, and maintenance of computing equipment and the contents therein.

P. **Unauthorized equipment or software modifications.** Users shall not add hardware and/or software to a computer, modify system files or settings, or delete standard software on a computer without prior approval of the IT Division. Unauthorized alterations to computers eventually result in lost productivity. Such changes often involve a technician to fix both the original problem, and the problem caused by the would-be technician. Poor documentation of the procedures performed, and the order in which they were completed further complicate unauthorized changes to computers. The IT Division will determine the use and specifications of all technology equipment used. Contact the Director of IT Customer Service to coordinate requests for new computing equipment and modifications.

Q. **Harassment.** Employees shall not access or send files, data, pictures, games, or jokes that contain pornographic, obscene or lewd material, derogatory remarks, slurs or gestures that demean, ridicule or torment an individual. Harassing behavior can create an intimidating, hostile or offensive work environment, thus making way for the College and the employee to incur legal liability. All violations shall be reported to your supervisor.

R. **Mobile devices/removable storage devices.** These devices provide excellent convenience for storage and transportation of data. The possibility of losing such a device puts the College and individuals at risk for data theft if personally identifiable information is stored on the device. Individuals should use a virtual private network (VPN) to access data stored by the College when working away from their desktop or at a remote location.

VI. **SOCIAL NETWORKING POLICY**

Students and higher education institutions are increasingly using social networking Web sites and on-line communities to communicate with each other and post events and updates. Refer to the Social Media Guidelines found on the Marketing & Outreach webpage for more information on disseminating official college information.

The absence of, or lack of explicit reference to a specific site does not limit the extent of the application of this policy. Where no policy or guideline exists, employees should use their professional judgment and take the most prudent action possible. Employees should consult their supervisor, Human Resources, IT or Community Relations & Marketing if uncertain how this policy applies.
A. College employees authorized by their departments may use approved social media or social networking sites to conduct College business in accordance with established guidelines. College social media pages or sites must be created and approved by Community Relations & Marketing. Publication guidelines for official college or department/organization social media content is similar to any other media. Oversight of all CTC-affiliated pages is the responsibility of the Office of Community Relations & Marketing, who will periodically review pages to ensure College policies are followed and that the pages are being produced in accordance with the best interests of the College.

B. Personal use of the College’s electronic resources to access social media and social networking sites is to be limited and must not interfere with an individual’s job performance or compromise the functionality of the campus network.

C. The College does not permit individuals or groups within the College community to present personal opinions in ways that imply endorsement by the College. Personal blogs should have clear disclaimers that the views expressed by the author in the blog is the author’s alone and do not represent the views of the College.

D. Be respectful to the College, other employees, students, vendors, and guests.

E. Employees’ online presence reflects the College. Employees should be aware that their actions captured via images, posts, or comments can reflect on the College.

F. Do not reference or cite faculty, staff, students, vendors, or guests without their express consent.

G. Respect copyright laws and reference cite sources appropriately. Plagiarism applies online as well.

VII. CONSEQUENCES OF MISUSE

Any employee found to have violated this policy will be subject to disciplinary action in accordance with the Human Resource Management Operating Policies and Procedures Manual up to and including termination of employment with CTCD.

VIII. DEFINITIONS

**Application.** A software program that serves a specific purpose for the user. Word processors, such as Microsoft Word®, are applications.

**Bandwidth.** The amount of data, measured in bits per second that can travel through a communications channel such as a network or modem.
Bit Torrent. Bit Torrent is a P2P file sharing protocol used for distributing large files such as movies and videos.

Chat. A real-time typed conversation that takes place on a computer.

Emoticon. “Smiley” keyboard letters and symbols used to show emotions in plain text messages.

Hacker. A person who tries to break the security of a computer or network.

Instant message (IM). A real-time Internet communications service that notifies a user when one or more people are online and then allows the user to exchange messages or files or join in a private chat room with those people.

Malicious code. Programs that can negatively affect a computer’s operation and capture information about a user, such as passwords and bank account information.

Marquee. Text animated to scroll across the screen. Often used as a screensaver.

Mobile device. Any pocket-sized computing device that has a small visual display screen for output and a miniature keyboard or touch screen for input.

Personally Identifiable Information. Information that can be used to identify, contact, or locate an individual. Names, addresses, and social security numbers are examples.

P2P. A peer-to-peer network on which users connect directly to each other’s hard disks and exchange files over the Internet. MP3 file-sharing applications are an example.

Removable storage devices. Storage devices used to store data and used for data transportation and/or data backup. USB Flash drives, cell phones, CDs, DVDs, and floppy disks are examples.

Shareware. Proprietary software that is provided to users free on a trial basis but may be limited in functionality, availability, or convenience with the understanding that the user may want to purchase it later. Shareware is available through download from an Internet Website or CD.

Software piracy. The illegal copying of computer software for distribution within an organization or distribution among friends and family without purchasing the appropriate amount of licenses.

Spam. The e-mail equivalent of junk mail that is unsolicited and usually unwanted by its recipients.
Spyware. Includes programs placed on a computer without the user’s knowledge and secretly collect information about the user. The program communicates information to an outside source while the user is online.

Streaming media. Streaming is the transfer of data in an even and continuous flow. Streaming media includes interactive and high-bandwidth applications, such as Internet radio.

Virtual Private Network (VPN). A private network over public network. A VPN provides users a secure channel between their home computer and a computer at a remote location.