

---

**SUBJECT:** Standing Operating Procedure| **DATE:** 04/18/2005

---

**NAME:** CTC Computer Usage Guidelines| **PAGE:** 1 of 11

---

## I. PURPOSE

This SOP 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 users, using property owned or operated by CTC, that 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, email messages, Internet usage, voice mail messages, and business telephone conversations on CTC equipment. CTC 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 so long as they are consistent with this policy statement.

## IV. 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.

**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.

---

**SUBJECT:** Standing Operating Procedure| **DATE:** 04/18/2005

---

**NAME:** CTC Computer Usage Guidelines| **PAGE:** 2 of 11

---

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

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.

Spam. The e-mail equivalent of junk mail that is unsolicited and usually unwanted by its recipients.

Spyware. Includes programs that are 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.

## V. USER RESPONSIBILITIES

All users of computing, networking, and other Information Technology 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);
- 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.

## VI. INAPPROPRIATE USES

(See the appendices of this policy; [Appendix A](#), IT Computer Usage – Threat Assessment Matrix, [Appendix B](#), Usage Statistics, [Appendix C](#), Laptop Checkout Contract and Guidelines, and Appendix D, Consequences of Misuse).

- 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 should be limited to those included with the Microsoft Windows® operating system.

---

**SUBJECT:** Standing Operating Procedure| **DATE:** 04/18/2005

---

**NAME:** CTC Computer Usage Guidelines| **PAGE:** 3 of 11

---

- B. Sending personal e-mail. 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 should only be used for the purpose for which they were created: College business communications.
- 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. An e-mail sent to everyone on the Outlook directory could be considered SPAM unless expressly authorized by the Central Texas College Director of Community Relations and Marketing or the Director of Student Life. 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 CTC website links to communicate general information rather than creating mass, campus-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, such as the HP3000, do not have unlimited resources. If a user logs into the HP3000 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. Use of instant messaging applications can seem easier and more convenient to use than the telephone or e-mail yet pose many risks to the College. Use of IM tools 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 using IM tools. Hackers posing as legitimate business contacts can steal confidential information.
- J. Chatting. See I, Using public IM tools.
- K. Downloading/installing unauthorized applications. Spyware can be loaded onto a computer when users download or install free screensavers or games. Spyware compromises user privacy by collecting information about your surfing habits and sending them over the Internet to third party software providers so that they can deliver advertising messages to you. Spyware can severely degrade the performance of your computer, add unnecessary traffic to the network and usurp Internet bandwidth.

---

**SUBJECT:** Standing Operating Procedure| **DATE:** 04/18/2005

---

**NAME:** CTC Computer Usage Guidelines| **PAGE:** 4 of 11

---

- L. Unauthorized use of confidential data. When a user obtains access to data on a system, they must safeguard that information by not sharing it with third parties. Failure to do so poses a major legal risk to the College.
- M. Downloading MP3 music. Peer-to-peer (P2P) file-sharing programs are used to illegally trade copyrighted music, movies, software, and games. P2P applications can leave a breach in an otherwise secure network. The amount of system resources required to download files will also cause slower Internet speeds. The software allows other users to share files on your hard drive, some of which may contain confidential information. The technology can be used as a means of transmitting computer viruses and worms. Many of the P2P programs contain spyware, allowing third parties to secretly gather information about users.
- N. 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.
- O. Maintaining confidential data on desktops. Unattended personal computers face exposure to theft and unauthorized access. Users should always logoff of their PCs when they are away from their desks. Laptops should not be left unattended and unsecured. Users should follow password guidelines, and install the latest software security updates. Any PC with sensitive data and information should be safeguarded to reduce the possibility of theft and the resultant legal risks to the College.
- P. 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 should be taken with respect to the operation, handling, and maintenance of computing equipment and the contents therein.
- Q. Unauthorized equipment or software modifications. Users should not add hardware 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 fixing 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. Requests for new computing equipment and modifications should be coordinated through the Director of IT Customer Service.
- R. Harassment. Employees should not send files, data, pictures, games, or jokes that contain 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 to incur legal liability. All violations should be reported to your supervisor.
- S. Playing/Downloading movies to DVD. See M, Downloading MP3 music.

---

**SUBJECT:** Standing Operating Procedure| **DATE:** 04/18/2005

---

**NAME:** CTC Computer Usage Guidelines| **PAGE:** 5 of 11



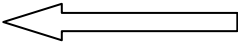
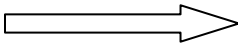
- T. Personalization. Employees should not personalize screen savers and email messages with signatures and quotes.

## VII. CONSEQUENCES OF MISUSE

- A. Any employee found to have violated this policy will be subject to disciplinary action in accordance with the Human Resources Management Operating Policies and Procedures Manual.
- B. See [Appendix D](#), **Consequences of Misuse**, for disciplinary actions for each offense. Violations not listed in this document will be handled case-by-case.
- C. Faculty, staff, and students of Central Texas College are expected to abide by local, state, and federal laws.

**Appendix A**

**Computer Usage Threat Assessment Matrix**

	<b>Level 3</b>	<b>Level 4</b>
 <b>High</b>	<ul style="list-style-type: none"> <li>● Unauthorized use of confidential data</li> <li>● Downloading/Installing unauthorized applications</li> <li>● Chatting</li> <li>● Using public IM tools</li> <li>● Listening to Internet radio</li> </ul>	<ul style="list-style-type: none"> <li>● Harassment</li> <li>● Unauthorized equipment or software modifications</li> <li>● Destroying equipment, information or data</li> <li>● Maintaining confidential data on the desktop</li> <li>● Playing computer games</li> <li>● Downloading MP3 Music</li> </ul>
<b>Low</b> 	<ul style="list-style-type: none"> <li>● Storing personal data on business computers</li> <li>● Sending personal email</li> <li>● Using emoticons, wallpaper and/or screensavers</li> <li>● Personalization</li> </ul>	<ul style="list-style-type: none"> <li>● Running two or more concurrent sessions</li> <li>● Sending chain letters</li> <li>● Web surfing</li> <li>● Generating spam</li> </ul>
	<b>Level 1</b>	<b>Level 2</b>
		
	<b>Low</b>	<b>High</b>
	<b>Impact on the System</b>	

**Level 1: Low.** Inappropriate use of college resources.

**Level 2: Moderate:** Potential to impede or cause damage to computing systems.

**Level 3: High.** Likely to impede or cause damage to computing systems.

**Level 4: Severe.** Will impede or cause damage to computing systems.

## Appendix B

### Usage Statistics

#### I. GENERAL ABUSE OF THE INTERNET

- Internet abuse at work is costing American companies more than \$85 billion annually in lost productivity. (*Websense, 2003*)
- 80 percent of companies stated that employees had abused Internet privileges. (*CSI/FBI Computer Crime and Security Survey, 2003*)

#### II. INSTANT MESSAGING

- Nearly 80 percent of instant messaging in companies is done over public IM services. (*Radicati, 2003*)
- There are more than 43 million users of consumer IM at work. (*IDC, 2003*)

#### III. P2P FILE SHARING

- Forty-five percent of the executable files downloaded through Kazaa contain malicious code. (*Trusecure, 2004*)
- More people looked for information about the P2P file sharing application Kazaa than any other topic on the Internet in 2003, according to search site Yahoo.<sup>1</sup>
- When a user downloads Kazaa, they also download spyware from third parties.<sup>2</sup>

#### IV. PORNOGRAPHY

- Seventy percent of porn is downloaded between 9:00 a.m. and 5:00 p.m. (*SexTracker*)

---

<sup>1</sup> <http://news.bbc.co.uk/2/hi/technology/3356397.stm>

<sup>2</sup> [http://www.kazaa.com/us/help/resource\\_usage.htm](http://www.kazaa.com/us/help/resource_usage.htm)

**SUBJECT:** Standing Operating Procedure| **DATE:** 04/18/2005

---

**NAME:** CTC Computer Usage Guidelines| **PAGE:** 8 of 11

---

**V. STREAMING MEDIA**

- Seventy-seven percent of weekly online listening to Internet Radio takes place between 5 a.m. and 5 p.m. Pacific time. (*Arbitron, 2004*)
- Forty-four percent of corporate employees actively use streaming media. (*Nielsen NetRatings, 2002*)

## Appendix C

### Laptop Checkout Contract and Guidelines

#### I. CHECKOUT CONTRACT

- A. Borrowers must sign a Laptop Checkout Contract and agree to abide by the usage guidelines contained in the CTC Computer Usage Guidelines document. Once checked out, a borrower assumes full responsibility for the laptop computer.
- B. Borrowers must provide a valid CTC Faculty or Staff ID.
- C. Borrower must pick up and return loaned equipment in the same condition.

#### II. USAGE AGREEMENT

Each Borrower must agree to these terms prior to checkout by signing a Laptop Checkout Contract and agreeing to follow computer care and maintenance guidelines.

- A. Laptops should be kept in a locked room or cabinet at all times. Never leave the laptop unattended. Never leave the laptop in a vehicle.
- B. Users should not store files on laptops. Files should be stored on storage media such as a CD.
- C. Do not touch the LCD screen with your hands or fingers.
- D. Do not subject the laptop to extreme temperatures. For example, do not leave the laptop in a hot car.
- E. Do not store your laptop, unused, for a long period of time. Humidity can damage the system in a closed environment, like a bag or closet.
- F. Do not twist or put tension on any of the cords or cables. Care should be taken with the network connector because it breaks easily.
- G. Users should not change any settings, load programs, or change components on any laptop computer.
- H. Use a surge protector.
- I. Do not use your laptop on your lap. A flat, solid surface is best.
- J. All laptops are warranted. If something goes wrong with the one you have borrowed, immediately contact the IT Help Desk.

**SUBJECT:** Standing Operating Procedure

| **DATE:** 04/18/2005

---

**NAME:** CTC Computer Usage Guidelines

| **PAGE:** 10 of 11

---

### **III. COMPUTER USAGE GUIDELINES**

In addition to the Laptop Checkout Guidelines, the Borrower agrees to adhere to Central Texas College's Computer Usage Guidelines.

### **IV. REPLACEMENT/DAMAGE CHARGES**

Negligence may result in the Borrower being responsible for covering the cost of lost or damaged technology equipment.

**SUBJECT:** Standing Operating Procedure| **DATE:** 04/18/2005**NAME:** CTC Computer Usage Guidelines| **PAGE:** 11 of 11**Appendix D****Consequences of misuse**

<b>Inappropriate Usages</b>		<b>Offense Escalation</b>			
		<b>Warning</b>	<b>Counseling</b>	<b>Reprimand</b>	<b>Dismissal</b>
<b>Level 1</b>	Using emoticons, wallpaper, screensavers, and/or marquee screensavers	X	X	X	X
	Sending personal email	X	X	X	X
	Storing personal data on college computers	X	X	X	X
<b>Level 2</b>	Generating SPAM	X	X	X	X
	Web surfing	X	X	X	X
	Sending chain letters	X	X	X	X
	Running two or more concurrent sessions	X	X	X	X
<b>Level 3</b>	Listening to Internet radio		X	X	X
	Using public IM tools		X	X	X
	Chatting		X	X	X
	Downloading/installing unauthorized applications		X	X	X
	Unauthorized use of confidential data		X	X	X
<b>Level 4</b>	Downloading MP3 music			X	X
	Playing computer games			X	X
	Storing confidential data on college computers			X	X
	Destroying equipment, information, or data			X	X
	Unauthorized equipment or software modifications			X	X
	Harassment			X	X