ACCEPTABLE TECHNOLOGY USE

SECTION 1. PREAMBLE

With the advent of powerful hardware and software, the Internet and the World Wide Web, computers have become a major communication tool. For example, we now use computers to send e-mail, explore the Web, gather information and offer distance learning. While computer use can stimulate intellectual, social and cultural growth, it can also facilitate harassment and other irresponsible, destructive behavior. The decentralizing power and flexibility a networked communications system affords may create situations that are not clearly covered by existing laws or current Contra Costa Community College District Policies or Procedures, making it mandatory that Contra Costa Community College District develop and enforce new policies and standards for the responsible use of technology on the campus. These policies, defining and governing acceptable and unacceptable use, will apply to anyone who uses any computer system, network system, Internet or Intranet web site, teleconferencing, or other data processing equipment owned or leased by Contra Costa Community College District as well as remote systems when used to access Contra Costa Community College District systems.

Use of the District's technology resources in violation of this procedure is prohibited, and may result in revocation of a user's access to the District's technology resources.

SECTION 2. DEFINITION OF TERMS

Administrative Officer:	Employee of Contra Costa Community College District with supervisory responsibility over a unit of the District which operates technology resources.
Computer Account:	The combination of a user number, user name, or user ID and a password that allows an individual access to a mainframe computer or some other shared computer or network.
Data Keeper:	The individual or department that can authorize access to information, data, or software and that is responsible for the integrity and accuracy of that information, data, or software. The Data Keeper can be the author of the information, data, or software or can be the individual or department that has negotiated a license for the District's use of the information, data, or software.
Information Resources:	In the context of this procedure, this phrase refers to data or information and the software and hardware that makes that data or information available to users.
Mainframe Computers:	"Central" computers capable of use by several people at once.
Network:	A group of computers and peripherals that share information electronically, typically connected to each other by either cable or satellite link.
Normal Resource Limits:	The amount of disk space, memory, printing, etc., allocated to your user account by that systems administrator.

Peripherals:	Special-purpose devices attached to a computer or computer network, (i.e., printers, scanners, plotters, etc.).
Project Director:	Person charged with administering a group of computer accounts and the computing resources used by the people using those computer accounts.
Server:	A computer that contains information shared by other computers on a network.
Software:	Programs, data, or information stored on removable media (tapes, disks, diskettes, cassettes, cds, etc.).
System Administrator:	Staff employed by Contra Costa Community College District whose responsibilities include system, site, or network administration and staff employed by Contra Costa Community College District departments whose duties include system, site, or network administration. System administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational. If you have a computer on your desk, you may be acting, in whole or in part, as that computer's system administrator.
Technology Resources:	The sum total of all computers, workstations, mainframes, software, cabling, telephone systems, video equipment, peripherals, networks, accounts, passwords, ID numbers, and data owned or leased by Contra Costa Community College District.
Voice Mail:	With the advent of enhanced phone systems, voice mail messages are stored as data files on a computer system.
User:	Someone who does not have system administrator responsibilities for a computer system or network but who makes use of that system or network. A user is still responsible for his or her use and for learning proper data management strategies.
User Account:	The combination of a user number, user name, or user ID and a password that allows an individual access to a mainframe computer or some other shared computer or network.

SECTION 3. PROCEDURE COVERAGE

Section 3.1 Access

Contra Costa Community College District is committed to providing access to computing resources to all current students and employees. While providing students and employees limited access to District computer resources is consistent with the education and service missions of the District, such access to this valuable and vulnerable district resource is a revocable privilege. Contra Costa Community College District is responsible for securing its network and computing systems to a reasonable degree against failure, loss of data, and unauthorized access while making them accessible to the largest possible group of authorized and legitimate users.

Section 3.2 Privileges

3.2.1 Technology provides access to District resources as well as the ability to communicate with others worldwide. Access to the District's technology resources is a revocable privilege which requires that users act responsibly and in a manner consistent with the provisions of this procedure and Board Policy.

3.2.2 Users do not own accounts on Contra Costa Community College District technology resources, but rather are granted the privilege of using such accounts. The District owns the account and grants individuals the privilege of using it.

3.2.3 All enrolled students and District employees may apply for user ID's to utilize e-mail and Internet and Intranet services offered by the District.

Section 3.3 Responsibilities

As a condition of the privilege of using Contra Costa Community College District's technology resources, each user will be held accountable for his or her own actions which affect such resources. A user who violates the terms of this procedure or said Board Policy shall be held responsible for his or her actions, and will be subject to revocation or suspension of his or her privilege of using the District's technology resources.

3.3.1 Contra Costa Community College District technology resources are to be used for District related research, instruction, learning, distribution of scholarly information, and administrative activities. Such uses shall be consistent with, and limited by the activities set forth in Section 4.1 [Appropriate Use] of this procedure. Users are required to use the District's technology resources, including hardware, software, networks, mailboxes and computer accounts in accordance with this procedure and in respect of the rights of other technology resource users. Contra Costa Community College District technology resources are not available and shall not be used for purposes specified in Section 4.2 of this procedure [Inappropriate Use].

3.3.2 Users shall not attempt to modify any system or network or attempt to crash or hack into Contra Costa Community College District systems. Users shall not tamper with any software protections or restrictions placed on computer applications or files. Unless properly authorized, users shall not attempt to access restricted portions of any operating system or security software. Users shall not attempt to remove existing software or add their own personal software to District computers and systems unless properly authorized.

3.3.3 Users shall use only their own designated accounts. Users are required to keep all ID's, passwords, and account information confidential, and shall take reasonable precautions to prevent others from obtaining this information. It is recommended that users change their passwords periodically to prevent unauthorized use of their account. Accounts are not transferrable, and users shall not allow others to use their own account. Users will be responsible for any use of their accounts by others to whom access has been given.

User's shall not use another individual's ID, password or account. Users shall respect the privacy and personal rights of others, and are prohibited from accessing or copying another user's e-mail, voice mail, data, or other files without the prior express consent of that user. Users shall send e-mail or voice mail only from their own personal addresses. Users are prohibited from concealing or misrepresenting their identity while using the District's computer resources.

3.3.4 Users are responsible for using software and electronic materials in accordance with copyright and licensing restrictions. Users are required to abide by all applicable copyright and trademark laws, and to abide by all licensing agreements and restrictions. Users shall not copy, transfer, or utilize any software or electronic materials in violation of such copyright, trademark, and/or licensing agreements. The copying of software that has not been placed in the public domain and distributed as "freeware" is expressly prohibited by this procedure. Users who access, copy, transfer and/or use "shareware" are expected to abide by the requirements of the shareware licensing agreement. No user may inspect, change, alter, copy, or distribute proprietary data, programs, files, disks or software without proper authority.

3.3.5 Users should remember that they are using Contra Costa Community College District technology resources and that this reflects upon the image of the District and not just an individual. Even with appropriate disclaimers, the Contra Costa Community College District is represented by its students and employees, and so appropriate decorum is warranted.

The principles of academic freedom apply in full to electronic communications. The conventions of courtesy and etiquette which govern vocal and written communications shall extend to electronic communications as well. Fraudulent, harassing, threatening, or obscene messages (as those terms are defined in Section 3.4.2.1.1 of this procedure) and/or other materials must not be transmitted through the District's technology resources.

3.3.6 Expected Privacy

Contra Costa Community College District's technology resources and all user accounts are the property of the District. There is no right to privacy in the use of the technology resources or user accounts, and the District reserves the right to monitor and access information on the system and in user accounts for the purpose of determining whether a violation of Board Policy or of this procedure has occurred. The District will remove any information on the system which it determines to be in violation of state or federal law, Board Policy or District Administrative Procedures.

Users must understand the weak privacy afforded by electronic data storage and electronic mail in general, and apply appropriate security to protect private and confidential information from unintended disclosure. Electronic data, including e-mail which is transmitted over the District's technology resources and/or the Internet is more analogous to an open postcard than to a letter in a sealed envelope. Under such conditions, the transfer of information which is intended to be confidential should not be sent through the Contra Costa Community College District's technology resources.

In addition, users should be aware that the Contra Costa Community College District may access information contained on its technology resources under numerous circumstances, including, but not limited to, the following circumstances:

Under the California Public Records Act (CPRA), electronic files are treated in the same way as paper files. Public documents are subject to inspection through CPRA. In responding to a request for information under the CPRA, the District may access and provide such data without the knowledge or consent of the user.

The Contra Costa Community College District will cooperate appropriately, upon the advice of District legal counsel, with any local, state, or federal officials investigating an alleged crime committed by an individual affiliated with a Contra Costa Community College District technology resource, and may release information to such officials without the knowledge or consent of the user.

The contents of electronic messages may be viewed by a system administrator in the course of routine maintenance, or as needed for Contra Costa Community College District administrative purposes, including investigation of possible violations of this procedure.

In addition, electronic and voice mail systems store messages in files (i.e., the file containing a user's inbound or saved mail). These files are copied to back-up tape in the course of system backups. The contents of these files and the copies on system backup tapes are subject to disclosure as stated in the preceding paragraphs.

3.3.7 Receipt of Offensive Material

Due to the open and decentralized design of the Internet and networked systems of the Contra Costa Community College District, the District cannot protect individuals against receipt of material that may be offensive to them. Those who use the Contra Costa Community College District's technology resources are warned that they may receive materials that are offensive to them. Likewise, individuals who use e-mail or those who disclose private information about themselves on the Internet or on Contra Costa Community College District technology resources should know that the District cannot protect them from invasions of privacy by third parties or other users.

Section 3.4 Ethical Standards

The Contra Costa Community College District's technology resources offer powerful tools for open learning and exchange of ideas. However, with power comes responsibility and ethical obligation. If this electronic medium of exchange is to function well and support an open, caring community of learners, its users need to agree to and abide by ethical standards of online behavior that assure all users full, equitable, effective and efficient access and use. Such ethical standards include but are not limited to:

3.4.1 Honesty:

3.4.1.1 Users agree to represent themselves according to their true and accurate identities in all electronic messages, files and transactions at all times.

3.4.1.2 While using Contra Costa Community College District technology resources, users agree to behave within the standards described in applicable college or District policies, procedures, or collective bargaining agreements.

3.4.2 Respecting Rights of Others:

3.4.2.1 Students and Employees.

3.4.2.1.1 Legal and ethical limitations on the use of District technology resources.

In using the District's technology resources, users must communicate in the same manner as is expected in the classroom or on campus. The distance provided by electronic communications does not create a forum in which there are no ethical or legal limitations. Users shall not use District technology resources in any unlawful manner including, but not limited to, attempting to defraud another, threatening physical harm to another, procuring or distributing obscene material in any form, or unlawfully harassing another.

While the District recognizes and respects users' rights to freedom of speech, such rights are not absolute. Speech which is fraudulent, libelous, obscene, harassing, or threatening is not permitted under state or federal law. Users are expressly prohibited from using the District's technology resources to engage in such conduct. Users violating this section will be subject to revocation of their user accounts and District technology resources.

For purposes of this procedure, the terms fraud and libel are given their legal meaning as developed by the courts of this State and of the United States. "Obscenity" means words, images or sounds which a reasonable person, applying contemporary community standards, when considering the contents as a whole, would conclude that they appeal to prurient sexual/physical interests or violently subordinating behavior rather than an intellectual or communicative purpose, and materials that, taken as a whole regarding their content and their particular usage or application, lack any redeeming literary, scientific, political, artistic or social value. "Threatening" means communications which result in an individual being fearful of imminent bodily harm and/or emotional/mental disruption of his/her daily life. "Harassing" means to engage in a knowing and willful course of conduct directed at another which seriously alarms, annoys or harasses another, and which serves no legitimate purpose. In addition, "Harassment" shall also mean to subject another to unwelcome sexual advances, requests for sexual favors, and other verbal, visual or physical conduct of a sexual nature as set forth in California Education Code Section 212.5.

3.4.2.2 Users shall have respect for the integrity and content of District electronic documents, records or IDs issued or posted online by employees.

3.4.2.3 Users shall have respect for the rights of others over the integrity of their intellectual property and to the fruits of their intellectual labor.

3.4.2.4 Users shall have respect for the access and security procedures and systems established to ensure the security, integrity and operational functionality of the District technology resources for the entire Contra Costa Community College District community.

SECTION 4. APPROPRIATE/INAPPROPRIATE USE OF DISTRICT COMPUTER RESOURCES

The Contra Costa Community College District's technology resources exist to support the instructional, cultural, research, professional and administrative activities of the Contra Costa Community College District community. In general, and unless otherwise specified herein, the same guidelines that apply to the use of all Contra Costa Community College District facilities apply to the use of the District's technology resources. All users are required to behave in a responsible, ethical and legal manner as defined by this procedure, and other existing Contra Costa Community College District policies and procedures. The following sections broadly define appropriate and inappropriate use.

Section 4.1 Appropriate Use

Activities deemed to be appropriate uses of Contra Costa Community College District technology resources include the following:

4.1.1 Educational Use (students)

Carrying out Contra Costa Community College District course assignments and activities requiring access to and use of campus technology resources, including:

4.1.1.1 Authorized access to and use of computer programs licensed by Contra Costa Community College District available on stand-alone and networked stations.

4.1.1.2 Authorized access to lab and campus networks to perform and complete required course work for Contra Costa Community College District courses in which the user is currently enrolled.

4.1.1.3 User access to authorized Contra Costa Community College District student e-mail accounts.

4.1.1.4 Independent study and research.

4.1.1.5 Agreement by user to follow acceptable use policies established by individual computing labs and network systems and to obey directives issued by authorized Contra Costa Community College District personnel supervising such labs and systems.

4.1.2 Instructional Use (faculty)

4.1.2.1 Use in classroom instruction.

4.1.2.2 Development of instructional materials.

4.1.2.3 Research connected to academic and instructional concerns and interests.

4.1.2.4 Communication with colleagues, students, and professional organizations and institutions if such communications are related to the business of the District.

4.1.3 Administrative Use (District employees)

4.1.3.1 District administrative and business communications and transactions.

4.1.3.2 Communication with colleagues, students, and professional organizations and institutions if such communications are related to the business of the District.

4.1.3.3 Research tied to District concerns and interests.

Section 4.2 Inappropriate Use

Use of District's technology resources for purposes other than those identified in Section 4.1 is not permitted. Users are specifically prohibited from using Contra Costa Community College District's technology resources in any manner identified in this section, as discussed in the following subsections.

Users who violate this section of the procedure by engaging in inappropriate use of the District's technology resources shall be subject to revocation or suspension of user privileges, student or employee disciplinary procedures, and may be subject to criminal or civil sanctions if permitted by law.

4.2.1 Destruction or damage to equipment, software, or data belonging to Contra Costa Community College District or others.

4.2.2 Disruption or unauthorized use of Contra Costa Community College accounts, access codes, or ID numbers.

4.2.3 Use of Contra Costa Community College District's technology resources to harass others, as defined in Section 3.4.2.1.1 of this procedure.

4.2.4 Use of Contra Costa Community College District's technology resources in ways which intentionally or unintentionally impede the computing activities of others are prohibited. Such activities include, but are not limited to: disrupting another's use of computer resources by game playing; sending an excessive number of messages or e-mail; making or printing excessive copies of documents, files, data, or programs; or intentionally introducing computer viruses of any type onto Contra Costa Community College District's technology resources.

4.2.5 Use of Contra Costa Community College District's technology resources which violate copyrights, trademarks, and or license agreements.

4.2.6 Use of Contra Costa Community College District's technology resources to violate another's privacy, including, but not limited to, accessing or using another user's account, ID number, password, electronic files, data, or e-mail.

4.2.7 Use of Contra Costa Community College District's technology resources in an effort to violate any District policy or procedure.

4.2.8 Specific examples of inappropriate use of technology resources include, but are not limited to:

4.2.8.1 Impersonation of any person or communication under a false or unauthorized name.

4.2.8.2 Transmission of any unsolicited advertising, promotional materials or other forms of solicitation.

4.2.8.3 Using Contra Costa Community College District resources for commercial purposes or personal financial gain.

4.2.8.4 Sending or storing messages and/or materials with the intent to defraud, harass, defame, or threaten.

4.2.8.5 Inappropriate mass mailing "spamming" or "mail bombing."

4.2.8.6 Tampering with any software protections or restrictions placed on computer applications or files.

4.2.8.7 Knowingly or carelessly introducing any invasive or destructive programs (i.e., viruses, worms, Trojan Horses) into Contra Costa Community College District computers or networks.

4.2.8.8 Attempting to circumvent local or network system security measures.

4.2.8.9 Altering or attempting to alter system software or hardware configurations on either network systems or local computing devices.

4.2.8.10 Installing unauthorized software programs on Contra Costa Community College District local computing devises or network systems and/or using such programs.

4.2.8.11 Ignoring or disobeying policies and procedures established for specific computer labs or network systems.

4.2.8.12 Copying system files, utilities and applications that expressly belong to the Contra Costa Community College District.

4.2.8.13 Surfing inappropriate non-work related websites such as those that are sexually explicit, gambling related or that subscribe to hate propaganda.

4.2.8.14 The use of chat rooms/messenger services for non-work related purposes is prohibited.

SECTION 5. INAPPROPRIATE USE OF CONTRA COSTA COMMUNITY COLLEGE DISTRICT TECHNOLOGY RESOURCES: REPORTING AND CONSEQUENCES

Section 5.1 Reporting Violations

Authorized system supervisors may informally resolve unintentional or isolated minor violations of use policies through e-mail or face-to-face discussion and education with the user or users concerned. For more serious violations, the following actions will be taken:

5.1.1 Student Violations

Individuals may report a suspected violation of this procedure by a student to the appropriate College Dean's Office. The Dean's Office shall then determine whether a violation of this procedure or of Board Policy has occurred. If the Dean's Office determines that a violation has occurred, the Dean's Office may take immediate action to suspend or revoke the user's privileges. In the event a user's privileges are suspended or revoked, the Dean's Office must provide the user with written notice of the suspension or revocation, and provide a statement of reasons for the actions taken. Possible sanctions include the deletion of materials found to be in violation of this procedure or of Board Policy, loss of user privileges, student expulsion, and other sanctions available within the judicial processes.

5.1.2 Employee Violations

Individuals may report a suspected violation of this procedure, or of Board Policy by District employees to the accused employee's supervisor who will immediately refer the complaint to District Human Resources for review. District Human Resources shall then determine whether a violation of this procedure or of Board Policy has occurred. If District Human Resources determines that a violation has occurred, they may contact the System Administrator to take immediate action to suspend or revoke the user's privileges. In the event a user's privileges are suspended or revoked, District Human Resources must provide the user with written notice of the suspension or revocation, and provide a statement of

reasons for the actions taken. District Human Resources may also make a determination of whether disciplinary action should be taken pursuant to established District collective bargaining agreements, Board policies, administrative procedures, and/or other applicable laws, rules or procedures. District Human Resources' determination to suspend or revoke an employee's user privileges may be appealed using the established grievance procedures applicable to the employee. Possible sanctions include deletion of material found to be in violation of this procedure and loss of technology resource user privileges. Other forms of employee discipline may be invoked under existing laws or Contra Costa Community College District policies and procedures.

Section 5.2. Investigating Violations

If Contra Costa Community College District staff or system administrators have information that a violation of this procedure, or of Board Policy, or any other misuse of technology resources has occurred, and if that information points to the activities or the computer files of an individual, they have the obligation to pursue any or all of the following steps to protect the user community:

- Take action to protect the system(s), user jobs, and user files from damage. Contra Costa Community College District reserves the right to immediately suspend a user's privilege of access to Contra Costa Community College District's technology resources if it has any reason to believe that the user has committed a violation of this procedure or of Board Policy.
- Notify the alleged abuser's supervisor, project director, instructor, academic advisor, or administrative officer, as appropriate, of the investigation.
- Refer the matter for processing through the appropriate Contra Costa Community College District disciplinary process.
- Suspend or restrict the alleged abuser's technology privileges during the investigation and administrative processing.
- Inspect the alleged abuser's files, diskettes, and/or backup tapes.
- Minor infractions of this procedure or those that appear accidental in nature are typically handled internally in an informal manner by electronic mail or in-person discussions. More serious infractions are handled via the procedures outlined above.
- Infractions such as harassment, or repeated minor infractions as described in this procedure may result in the temporary or permanent loss of user privileges, notification of a student's academic advisor and/or Dean's Office, or the appropriate supervisor and District Human Resources in the case of an employee.
- More serious infractions, such as unauthorized use, attempts to steal passwords or data, unauthorized use or copying of licensed software, violations of Contra Costa Community College District's policies or procedures, or repeated violations of minor infractions may result in the temporary or permanent loss of technology resource privileges.
- Offenses which are in violation of local, state, or federal laws may result in the immediate loss of technology resource privileges, and will be reported to the appropriate law enforcement authorities.