Book	Administrative Procedures
Section	Chapter 3: General Institution
Title	Computer and Network Usage
Code	AP 3720
Status	Active
Adopted	July 21, 2004
Last Revised	December 17, 2007

Reference: Education Code Section 70902; 17 U.S.C. Section 101 et seq.; Penal Code Section 502, Cal. Const., Art. 1 Section 1; Government Code Section 3543.1(b), Federal Rules of Civil Procedure, Rules 16, 26, 33,34,37,45.

The Board of Trustees, in granting access to District computers and networks, expects that employees and students, in their use of these systems, will adhere to legal and ethical standards consistent with the District's mission.

Administration has developed the following regulations and procedures setting forth the specific responsibilities and obligations related to use of District computers and networks. Disciplinary procedures to enforce this agreement have been established that are consistent with policies and laws governing the conduct of employees and students.

Computer and Network Usage Regulations

1. PURPOSE

This is a District-wide agreement for all sites of the Yuba Community College District (District) to allow for the proper use and management of all College computing and network resources. Those District sites and departments that operate separate networks or systems may add individual guidelines that supplement, but do not relax, this agreement.

The District grants access to its networks and computer systems subject to certain responsibilities and obligations set forth herein and subject to all local, state, and federal laws. Appropriate use should always be legal, ethical and consistent with the District's mission.

The District grants access to its networks and computer services to facilitate its educational mission. Authorized users are granted the privilege of use to support the educational activity of the District. Research, scholarly communication, administrative activity, and interaction with students, faculty, staff and administrators throughout this District and throughout the world are appropriate when conducted in accord with the mission of the District.

The District electronic mail and other network services may be used for incidental personal purposes provided that, in addition to all other conditions and restraints stated in this agreement, such use does not directly or indirectly interfere with the District operation of its computing network and services, burden the District with noticeable incremental cost, or interfere with the user's employment or other obligations to the District.

2. AUTHORIZED USE

Authorized use of District-owned or operated computing and network resources is use consistent with this agreement. An Authorized User is any person who has been granted authority by the District to access its computing and network systems and whose usage complies with this agreement. Authority to use a particular District computing or network resource should come from the campus unit responsible for operating the resource. Unauthorized use is strictly prohibited. The terms "Authorized User" and "user" are hereinafter used interchangeably.

3. PRIVACY

Users must recognize that there is no guarantee of privacy associated with their use of District network and computer systems. The District may find it necessary to view electronic data in order to properly administer the system or in order to investigate a complaint. The District may also be required by law to allow third parties to view files, data and messages (e.g. electronically stored data may become evidence in legal proceedings, or subject to Public Records Act disclosure requirements.) It is also possible that messages or data may inadvertently be viewed by others.

4. INDIVIDUAL RESPONSIBILITIES

4.1. Common Courtesy and Respect for Rights of Others
All users are responsible to respect and value the privacy of others, to behave ethically, and to comply with all legal restrictions regarding the use of electronic data. All users are also responsible to recognize and honor the intellectual property rights of others. Communications on District computers or networks should be businesslike, courteous and civil. Such systems must not be used for the expression of animus or bias against individuals or groups, offensive material such as obscenity, vulgarity or profanity, inappropriate jokes or other non-businesslike material. Users who engage in such activity will be subject to disciplinary action.

No user may, under any circumstances, use District computers or networks to libel, slander, or harass any other person. The following are examples of Computer Harassment: (1) intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to

communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); (4) intentionally using the computer to disrupt or damage the academic, research, administrative, or related pursuits of another; or (5) intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of the privacy of another.

No user shall use the system to send excessive amounts of email or generate excessive amounts of traffic on another system, and shall not: (1) forge email or USENET posting header information, (2) send large numbers of unsolicited mail messages, (3) add addresses to any mailing list without explicit positive consent of the addressee, (4) forwarding or posting of chain letters, (5) or engage in harassment, whether through language, frequency, or size of messages.

Nondiscrimination. All users have the right to be free from any conduct connected with the use of Yuba Community College District network and computer resources which discriminates against any person on the basis of BP 3410-Nondiscrimination. No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District procedure regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

4.2. Responsible Use
All users are responsible for refraining from all acts that waste District computer or network resources or prevent others from using them. Each user is responsible for the security and integrity of information stored on his/her personal desktop system. Computer accounts, passwords, and other types of authorization are assigned to individual users and must not be shared with or used by others. All users must maintain confidentiality of student information in compliance with the Family Educational Rights and Privacy Act of 1974 and the California Education Code as interpreted in the Student Records Policy.

In addition, all users are responsible to exercise judgment in the use of the access the District network provides to external networks (the Internet). Users are advised that on the Internet they may encounter material which may be considered offensive or objectionable in nature or content. Users are further advised that the District does not assume responsibility for the content on any
outside network.

4.2.1. Permitting unauthorized access
All users are prohibited from running or otherwise configuring software or hardware to intentionally allow access by unauthorized users.

4.2.2. Use of privileged access
Special access to information or other special computing privileges are to be used in the performance of official duties only. Information that is obtained through special privilege is to be treated as private.

4.2.3. Termination of access
Whenever a user ceases being a member of the District community or if such user is assigned a new position and/or responsibilities within the District, such user shall not use facilities, accounts, access codes, privileges, or information for which he/she is not authorized in his/her new position or circumstances.

4.3. Attempts to circumvent security
Users are prohibited from attempting to circumvent or subvert any security measures implemented for the District computing and network systems. The use of any computer program or device to intercept or decode passwords or similar access control information is prohibited. This section does not prohibit use of security tools by Information Technologies personnel.

4.3.1. Denial of service
Deliberate attempts to degrade the performance of a computer system or network or to deprive authorized users of access to or use of such resources are prohibited.

4.3.2 Harmful activities
The following harmful activities are prohibited: creating or propagating viruses; disrupting services; damaging files; intentional destruction of or damage to equipment, software or data belonging to the District and the like.

4.3.3 Unauthorized access
All users are also strictly prohibited from: (1) damaging computer systems; (2) obtaining extra resources without authority; (3) depriving another user of authorized resources; (4) sending frivolous or excessive messages (e.g. chain letters); (5) gaining unauthorized access to District computing and networking systems; (6) using a password without authority; (7) using loopholes in the District computer security systems without authority; (8) using another user's password; and (9) accessing abilities used during a previous position at the District.

4.3.4 – Unauthorized Computer Connection
No one shall connect any computer to any of the District networks unless it meets technical and security standards set by the District administration.

The applicable requirements depend on what kind of connection is being made. For example, dialing up with an ordinary asynchronous modem or accessing the internet via a Wi-Fi hot spot does not require any special authorization, but connecting to the campus-wide Ethernet cable does, because one improperly configured machine on a network can cause widespread disruption.

4.4. Use of licensed software
No software may be installed, copied, or used on District resources except as permitted by the owner of the software and by law. Software subject to licensing must be properly licensed and all license provisions (installation, use, copying, number of simultaneous users, term of license, etc.) must be strictly adhered to. District software will only be installed on District computers to ensure these provisions are met. In addition, District computers will only have District software installed on them.

4.5. Personal business, political campaigning, and commercial advertising
The District's computing and network systems are a District-owned resource and business tool to be used only by authorized persons for District business and academic purposes. Except as may be authorized by the District, users should not use the District's computing facilities, services, and networks for (1) compensated outside work; (2) the benefit of organizations not related to the District, except in connection with scholarly pursuits (such as faculty publishing activities); (3) political campaigning; (4) commercial or personal advertising; (5) the personal gain or benefit of the user.

4.6 – World Wide Web Publishing
Those who publish World Wide Web pages or similar information resources on District computers shall take full responsibility for what they publish; shall respect the acceptable-use conditions for the computer on which the material resides; shall obey all applicable laws; and shall not publish commercial advertisements without prior authorization. References and links to commercial sites are permitted, but advertisements, and especially paid advertisements, are not. Users shall not accept payments, discounts, free merchandise or services, or any other remuneration in return for placing anything on their web pages or similar facilities. Web pages on the District's network are subject to the same rules as other uses of the same

facilities. Different District computers are set up for different purposes; some do not permit individual Web pages at all. On other District computers, individuals are allowed to set up Web pages to pursue personal interests, but even then, the available disk space and communication bandwidth are limited. System administrators can advise about what is permitted at any particular site.

4.6.1 – Individual Responsibility
When you publish something on the World Wide Web, you are putting it before a potential audience of millions. You have the same responsibilities as if you were publishing a newspaper. If the content is libelous or deceptive, people can sue you and you can be held personally liable.

4.6.2 - Obscene Material
Since there are laws against distributing obscene material (not just creating it), a link to an obscene web site can be a violation of the law. This is true regardless of the status of the Communications Decency Act or other new laws that specifically mention computers. There is no District rule that prohibits you from viewing any web page anywhere. However, the District's sexual harassment policy prohibits you from displaying sexually explicit material which interferes with anyone's work or academic performance or creates an intimidating, hostile, or offensive working or academic environment. That is why many campus computer labs do not permit the display of erotic images on screens visible to others.

4.6.3 – Copyright Permission
If you want to reproduce copyrighted pictures, cartoons, or comic strips on your web page, you must have the copyright owner's permission. It is not sufficient to reproduce the owner's copyright notice; you must actually obtain permission for yourself, just as if you were publishing the same material in a newspaper. Brief textual quotations do not always require permission as long as the source is acknowledged and you are not reproducing a complete work (poem, essay,
etc.).

4.6.4 – Business/Advertising Links
You are welcome to include links to businesses and commercial sites for their information value, as long as your links do not constitute advertisements. If you are personally connected with an outside business, you may mention the connection briefly on your District web page so that people who are looking for you can find you. (For example, authors of books can include links to their publishers; consultants can include links to their consulting firms; and District units can advertise publications, software, and similar materials produced in connection with their work.) However, you must not solicit outside business or publish commercial advertisements or advertising graphics on a District computer.

4.6.5 – Web Services and Electronic Commerce
You must not accept payments, discounts, or anything of value in return for placing anything on your web page. The District's disk space and communication capacity are not yours to sell. This applies to all computers directly connected to the District's network cables, even if they are privately owned.

A few District sites, such as the bookstores, may be authorized to publish paid advertising for outside clients as part of their official function. Because it imposes costs on the whole District network, this activity must be cleared with the Board, not just system administrators or department heads.

5. SECURITY

5.1. System administration access
Certain system administrators of the District's systems will be granted authority to access files for the maintenance of the systems, and storage or backup of information.

5.2. District Access
The District may access usage data, such as network session connection times and endpoints, CPU and disk utilization, security audit trails, network loading, etc. Such activity may be performed within the reasonable discretion of the Information Technologies management, subject to District approval.

5.3. Departmental responsibilities
Each District department has the responsibility of: (1) enforcing this agreement; (2) providing for security in such department area; (3) providing authorized users within the department with resources for regular disk backups (software, hardware, media, and training); and (4) providing for virus protection.

5.4. Public information services
Departments and individuals may, with the permission of the Director Information Technologies of the District, configure computing systems to provide information retrieval services to the public at large under the auspices of the District. (Current examples include "anonymous ftp," "gopher," and "World Wide Web.") However, in so doing, particular attention must be paid to issues addressed earlier in this agreement, such as authorized use, responsible use of resources and individual and departmental responsibilities. In addition, copyrighted information and materials and licensed software must be used in an appropriate and lawful manner.

6. PROCEDURES AND SANCTIONS

6.1. Responding to security and abuse incidents
All users and departmental units have the responsibility to report any discovered unauthorized access attempts or other improper usage of District computers, networks, or other information processing equipment. If a security or abuse problem with any District computer or network facility is observed by or reported to a user, such user shall immediately report the same to such user's department head and/or the Director Information Technologies.

6.2. Range of disciplinary sanctions
Minor infractions of this agreement, when accidental, such as consuming excessive resources or overloading computer systems, are generally resolved informally by the unit administering the accounts or network. This may be done through electronic mail or in-person discussion and education.

Repeated minor infractions or misconduct that is more serious may result in the temporary or permanent loss of computer access privileges or the modification of those privileges. More serious violations include, but are not limited to unauthorized use of computer resources, attempts to steal passwords or data, unauthorized use or copying of licensed software, repeated harassment, or threatening behavior. Offenders may be referred to their supervisor, sponsoring advisor, department, employer, or other appropriate District office for further action. If the offending individual is a student, the matter may be referred to the college/campus Chief Student Services Officer for disciplinary action.

Any offense that violates local, state, or federal laws may result in the immediate loss of all District computing privileges and will be referred to appropriate District offices and/or law enforcement authorities.

Note: It is the intention of the Technology Subcommittee in adopting this agreement, that it should be reviewed annually by the Subcommittee.

Appendix A

Conduct which violates this agreement includes, but is not limited to the activities in the following list:

• Unauthorized use of a computer account.

• Using the District Network to gain unauthorized access to any computer systems.

• Connecting unauthorized equipment to the District network. This does not pertain to those computers accessing the internet from a Wi-Fi hot spot.

• Unauthorized attempts to circumvent data protection schemes or uncover security loopholes. This includes creating and or running programs that are designed to identify security loopholes and or decrypt intentionally secure data.

• Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.

• Knowingly or carelessly running or installing on any computer system or network, or giving to another user a program intended to damage or to place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan Horses, and worms.

• Deliberately wasting/overloading computing resources, such as printing too many copies of a document.

• Violating terms of applicable software licensing agreements or copyright laws.

• Violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, etc.

• Using District resources for commercial activity such as creating products or services for sale.

• Using electronic mail to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.

• Initiating or propagating electronic chain letters.

• Inappropriate mass mailing. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing."

• Forging the identity of a user or machine in an electronic communication.

• Transmitting or reproducing materials that are slanderous or defamatory in nature, or that otherwise violate existing laws or District regulations.

• Displaying obscene, lewd, or sexually harassing images or text in a public computer facility or location that can be in view of others.

• Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

Revised: 12/17/2007; 12/01/2006; 1/03/2005
Adopted: 7/21/2004