| | | | | |
|---|---|---|---|---|
| Policy Change | ☒ | Subject Matter Area Review | ☒ | KEY: |
| Procedure Change | ☒ | Constituency Group Review | ☒ | BOLD= new language |
| New Policy | ☐ | District Council | ☐ | ~~strikethrough~~= delete language |
| New Procedure | ☐ | Board 1st Reading | ☐ | |
| | | Board 2nd Reading | ☐ | |
| Comments: | | Referred to: | | Edited: |
| CCLC Fall 2015 Update | | | | 12/16/15 |

**Yosemite Community College District** Policies and Administrative Procedures **No. 3720**

## Policy

## 3720 Computer and Network Use

Employees and students who use ~~d~~**D**istrict computers and networks and the information they contain, and related resources have a responsibility not to abuse those resources and to respect the rights of others. The Chancellor shall establish procedures that provide guidelines to students and staff for the appropriate use of information technologies. The procedures shall include that users must respect software copyrights and licenses, respect the integrity of computer-based information resources, refrain from seeking to gain unauthorized access, and respect the rights of other computer users.

**References:**
Education Code Section ~~70902(b)(3)~~ **70902; Government Code Section 3543.1(b); Penal Code Section 502; Cal. Const., Art. 1 Section 1; 17 U.S. Code Sections 101 et seq.**; ~~Title 5, Sections 55020 et seq., 55030 et seq., 55040 et seq.~~

**Adopted:** June 28, 2004
**Revision Adopted:** February 11, 2009
**Last Reviewed:**

**Administrative Procedure**

# 3720 Computer and Network Use

## I. Definitions

1. District Network

A variety of information technology resources, including computer and communication systems, providing voicemail, electronic mail (e-mail), telephone, and access to the Internet, are owned and operated by the District for the use of District faculty, administrators, staff, and students in support of the programs of the Colleges and District. These resources and all the component parts are referred to as the "District Network."

2. Ownership

The entire District Network, and all hardware and software components within it, is the sole property of the District, which for that reason has and retains complete and sole authority over the terms and conditions of its use. Except as provided in Board Policy or collective bargaining agreements pertaining to intellectual property rights, employees and students have no rights of ownership to these systems or to the information they contain by virtue of their use of all or any portion of the District Network.

3. Privacy

The District recognizes the privacy interests of faculty, ~~and~~ staff, **and students** and their rights to academic freedom, shared governance, and freedom of speech, as well as their rights to engage in protected union and concerted activity. However, both the nature of electronic communication and the public character of District business make electronic communication less private than many users may anticipate.

The District Network is not to be relied upon as confidential. All users of the District Network, including employees, students, independent contractors, and authorized guests, can have no expectation of privacy concerning their uses of the District Network or concerning information created or stored in such media. Nevertheless, the District does not routinely inspect, monitor or disclose such information without the user's consent.

**4. Malware**

**An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.**

## II. District Access

Because the District Network is solely owned and controlled by the District, system administrators may access user files or suspend services they manage without notice as required: (1) to protect the integrity of computer systems; (2) when required by and consistent with the law; (3) under time-dependent, critical operational circumstances; or (4) when there is a reason to believe that violations of law or District policy or procedures have occurred.

For example, system administrators, following organizational guidelines, may access or examine files or accounts that are suspected of unauthorized use or misuse or that have been corrupted or damaged. The District will attempt to notify users before discontinuing service. However, the District is not required to give notice or to show cause before accessing the District Network or any parts thereof.

## III. Acceptable Use

For District employees, the intended uses of the District Network are those which are reasonable and necessary for the pursuit of job duties; for students, the intended uses are those which are reasonable and necessary for the pursuit of instructional activities. Unauthorized uses include prohibited uses and any other use for a prohibited purpose, including illegal activities, messages which may constitute discrimination or harassment under state or federal law or anything that interferes with the intended use. These types of prohibited uses and purposes are further defined below.

## IV. Prohibited ~~u~~Use

Examples of behaviors constituting prohibited use or abuse which violate District Board Policy ~~2~~**3**720 include, but are not limited to, the following activities:

### A. System ~~a~~Abuse

- Using the telephone, voice mail or computer account without authorization.
- **Obtaining a password or access to an account that one is not authorized to have and/or knowingly or carelessly allows someone else to gain access to your account or escalated privileges to any other account** ~~Obtaining or using a password for a computer account that one is not authorized to have or use~~.
- Using the District Network to gain unauthorized access to any computer systems.
- Deliberately performing an act which will interfere with the normal operation of computers, terminals, peripherals or networks.
- Knowingly 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 **Malware** ~~computer viruses, Trojan horses and worms~~.
- Attempting to circumvent data protection schemes or uncover or exploit security loopholes.
- Violating terms of applicable software licensing or copyright laws.

- Masking the identity of an account or machine.

- Forging a name to an email, discussion group, web page or other electronic resource.

- Posting materials that violate existing laws on any college electronic resource.

- Attempting without District authorization 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 that user, or any activity which is illegal under California Computer Crime Laws.

- Using YCCD resources for personal gain or partisan political activity.

- Copying of copyrighted software.

- Deliberately wasting computing resources.

- Deliberately downloading, displaying, uploading or transmitting obscenity or pornography, as legally defined.

- Allowing someone else to use your account **or system access** who **views or modifies or deletes any information or** engages in any misuse in violation of Board Policy 3720 or of these procedures.

- Personal use which is excessive or interferes with the user's or others' performance of job duties, or otherwise burdens the intended use of the Network.

**B. Harassment**

- Using the telephone, e-mail or voice mail to harass or threaten others.

- **Sending defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information.**

- Knowingly downloading, displaying or transmitting by use of the District Network, communications, pictures, drawings or depictions that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political belief.

- Knowingly downloading, displaying or transmitting by use of the District Network sexually explicit images, messages, pictures, or cartoons when done to harass or for the purposes of harassment.

- Knowingly downloading, displaying or transmitting by use of the District Network sexually harassing images or text is prohibited.

- Posting on electronic bulletin boards**, websites or social media** material that violates existing laws or the colleges' Codes of Conduct.

- Using the District Network to publish false or defamatory information.

**C. Commercial ~~u~~Use**

- Using the District Network for any commercial activity, without written authorization from the District. "Commercial activity" means for financial remuneration or designed to lead to financial remuneration.

**D. Copyright**

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

- Publishing copyrighted material without the consent of the owner on District Web sites in violation of copyright laws.

## V. Exceptions

Activities by technical staff, as authorized by appropriate District or college officials, to take action for security, enforcement, technical support, troubleshooting or performance testing purposes will not be considered abuse of the Network.

Although personal use is not an intended use, the District recognizes that the Network will be used for incidental personal activities and will take no disciplinary action provided that such use is within reason and provided that such usage is ordinarily on an employee's own time; is occasional and does not interfere with or burden the District's operation. Likewise, the District will not purposefully survey or punish reasonable use of the network for union business-related communication between employees and their unions.

## VI. Enforcement

Abuse of computing, networking or information resources contained in or part of the District Network may result in the loss of computing privileges. Additionally, abuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under applicable District or college policies, procedures, or collective bargaining agreements. Complaints alleging abuse of the District Network will be directed to those responsible for taking appropriate disciplinary action. Illegal reproduction of material protected by U.S. Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment.

## VII. Disclosure

### A. Possibility of Disclosure

**Users must be aware of the possibility of unintended disclosure of communications.**

### B. Retrieval

**It is possible for information entered on or transmitted via computer and communications systems to be retrieved, even if a user has deleted such information.**

**C. Public Records**

**The California Public Records Act (Government Code Section 6250 et seq.) includes computer transmissions in the definition of "public record" and nonexempt communications made on the District network or computers must be disclosed if requested by a member of the public.**

**D. Litigation**

**Computer transmissions and electronically stored information may be discoverable in litigation.**

**References:**
**17 U.S. Code Sections 101 et seq.; Penal Code Section 502; Cal. Const., Art. 1 Section 1; Government Code Section 3543.1(b); Federal Rules of Civil Procedure, Rule 16, Rule 26, Rule 33, Rule 34, Rule 37, and Rule 45**

---

**Procedure Last Revised:** May 10, 2006
**Last Reviewed:**