

## **AP3720 Computer and Network Use**

District computer users have privileged access to:

- 1) Electronic mail communication with people all over the world.
- 2) The World-Wide Web and the information contained therein.
- 3) Internet and Intranet Discussion groups.
- 4) College Library Catalogs, the Library of Congress, online databases, etc.

All computers are to be used in a responsible, efficient, ethical and legal manner. The District does not and shall not inspect or monitor computers and computer-related matter, including but not limited to equipment, software, websites, hardware or related matter which is not owned by the District except as needed to prevent malware and protect the District Network. Violations of any of the procedures set forth below will be dealt with in the same manner as violations of other District policies and may also result in the temporary or permanent loss or modification of computer account and resource access privileges, and/or civil or criminal legal action.

### **3720.1 Acceptable Uses:**

- Conducting the business of the District.
- Developing and preparing classroom material.
- Communication and exchange for professional development, to maintain currency, or to debate issues in a field or sub field of knowledge.
- Research and instructional activities.
- Applying for or administering grants or contracts for research or instruction.
- Any other administrative communications or activities in direct support of research and instruction.
- Announcements of new products or services for use in research or instruction, but not advertising of any kind.
- Personal use of District electronic mail and computer services used for personal purposes provided that such use does not directly interfere with the District operation of computer facilities or electronic mail services, and provided that such use does not interfere with job requirements or work performance.

### **3720.2 Unacceptable Uses:**

- Accessing computers, accounts or folders, other than your own, except those specifically authorized by your supervisor or District ITSS.
- Intruding into any system in such a way as to diminish the effectiveness of system performance.
- Use for private for-profit activities.
- Advertising of products or services.

### **3720.3 E-mail**

The e-mail at SJECCD is here to provide a convenient way of communicating among students, faculty, staff, administrators and professional colleagues. It is expected that SJECCD computer users will use common courtesy in the use of e-mail. Specifically, the following activities are not acceptable:

- Hate mail, harassment, discriminatory remarks and other antisocial behaviors. Messages should not contain profanity, obscene comments, sexually explicit material, or expressions of bigotry or hatred.
- E-mail that is not District business such as "Chain letters," "broadcasting" messages to lists or individuals, and other types of use which would cause congestion of the networks or otherwise interfere with the work of others.

#### **3720.4 Software Licensing**

All commercial software used on college computers must be licensed to the college or to the individual who is using the software. All software should be assumed to be commercial unless otherwise noted. The District has the capability and reserves the right to electronically review and update the software installed on all District computers

Software protected by copyright may not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software may not be copied into, any District equipment or system, except pursuant to a valid license or as otherwise permitted by copyright law.

##### **A. District-wide Software Licenses**

SJECCD has obtained favorable site licenses for many products, including MS Office Suite, MS operating systems, Datatel, and virus protection software. For a list of software that is licensed to the District see the ITSS & CTSS offices.

##### **B. Departmental Software Licenses**

In order to maintain consistency and receive the best possible discounts, the ITSS & CTSS departments will purchase and load a set of standardized programs on all District computers. Individual departments can purchase specialized software for use by the employees of that department on a limited basis provided this is coordinated with the ITSS & CTSS departments. License information should be kept in the departmental office and be available for examination if required by a college, district or law enforcement official.

##### **C. Individual Software Licenses**

The District is responsible for providing access to all software necessary in the performance of an employee's required duties.

From time to time faculty may need to install software on their primary computer. This software must be licensed to the individual or the department. All appropriate license fees should be paid. This software must be reported to the appropriate departmental manager. Students shall not be permitted to install software on District computers.

Any fines levied for pirated software will be paid by the individual(s) who installed and/or knowingly used the pirated software in question on a District computer.

#### **3720.5 Security**

Security on any computer system is a high priority, especially when the system involves many users. If any employee believes there is a security problem on any of the District computers, the system administrator in ITSS should be notified immediately. Do not demonstrate the problem to other users.

**A. Usernames, Passwords, Personal Identification Numbers (PINS)**

Persons using the District's networks may be issued usernames, passwords and/or PINS. These ID's:

- 1) Are unique to the individual and should be guarded carefully.
- 2) Give the user of the ID access to certain data, files, information and resources within the District's electronic resources.
- 3) Will be treated as electronic signatures and carry the same authority as a written signature when used in conjunction with District or college documents, screens, telephone systems or web forms.

If a user believes someone else is using his/her ID, they should contact the systems administrator immediately.

**B. Data Security**

- Users shall not misrepresent other users on the network.
- Users shall not attempt to gain unauthorized access to data, information, system programs or computer equipment.
- Users must not give their password to another user.
- Users should change passwords per the recommended guidelines.

**C. Network Security**

Network Security is and should be the responsibility of every individual who uses the District's computer resources. All managers and technical employees should be especially aware of the possible vulnerabilities. ITSS is responsible for maintaining security through the issuing of passwords, and administration of all access points into the "Secured" network. No deviations should be made to these security measures without the written permission of the Director of ITSS or his/her designee.

The following guidelines help ensure that only authorized users will have access to the College and District's secured data.

- 1) The network backbone serving the colleges has been divided into two different and distinct networks: the Admin Network (Secured) and the Student Network (Unsecured).
- 2) All computers regularly used by students of the Colleges or accessible to the general public are and should be placed in the Student Network. These computers and their authorized users have access to the various web servers, academic support software, faculty distribution files, etc.
- 3) All computers regularly used by employees of the District, and not generally available for student use, should be and are placed in the Admin Network. These computers and their authorized users have physical access to campus e-mail systems, file servers, print servers and the central databases (Student Information System).
- 4) All employees of the District who make regular use of the computer systems are issued passwords to the network. These passwords should be treated as confidential and never released to anyone.
- 5) If someone who is not a regular employee of the District (e.g. student workers) has need of a password, this authorization can be provided by a District/college manager AND the Director of ITSS.

### **3720.6 Privacy**

Users should be aware that their electronic communications can come under scrutiny under certain provisions of California law and therefore should use good judgment and common courtesy in using these systems. The California Public Records Act (Government Code Sections 6250 *et seq.*) includes computer transmissions in the definition of “public records” and nonexempt communication made on the District network and computers must be disclosed if requested by a member of the public.

Pursuant to the terms of this policy, the District reserves the right to monitor all use of the District network and computers for legitimate District purposes, including but not limited to ensuring compliance with policy and procedure, and to protecting the integrity and security of the system. In keeping with its commitment to academic freedom and respect for privacy, the District will monitor its network and computers using the least intrusive means possible to accomplish such purposes.

These guidelines do not address the ownership of intellectual property /copyright stored on or transmitted through the District electronic communication resources. See SJECCD/FA, AFT 6157 Contract-Article 4.

The District may inspect, monitor, and disclose an individual’s electronic records only when one of the following conditions is met:

- 1) An employee’s written permission is obtained by the District prior to any access for the purpose of examination or disclosure
  - A search warrant has been issued permitting the inspection.
  - Examination and disclosure without the holder’s consent shall be limited to only those communications required by law, relevant to specific violations of policy, or necessary to critical time-dependent operations.
- 2) The District shall not inspect any personal material saved, stored, retained, or distributed by said computer or equipment without a search warrant in accordance with judicial safeguards, and all employees have an expectation of privacy in their personal materials.
- 3) The District will issue, in a manner consistent with law, an annual report to the FA, AFT 6157 summarizing instances of non-consensual examination or disclosure of electronic communications regarding faculty members without revealing personally identifiable data.

Users should be aware that:

- 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.
- ITSS employees who operate the system have the ability to access all files stored on the District’s servers. Such access shall be done only in accordance with the terms set forth in this Computer and Network Use Policy and Procedures. (See 3720.5 Privacy,.)
- Computer transmissions and electronically stored information may be discoverable in litigation and in any other proceeding that allows for formal discovery.

### Privacy of Use

The District acknowledges that due to the nature of the relationship between the District and the recognized employee unions on personnel disputes and bargaining matters, those unions and their members will have an expectation of privacy with respect to the content of their email communications involving such matters to the extent permitted by law. The District also acknowledges that faculty members have an expectation of privacy with respect to the content of email communications transmitted to students in the performance of teaching duties, pursuant to the terms of the District's contract with the Faculty Association.

The District shall follow the requirements of union contracts concerning disciplinary actions whenever consideration is being given to any kind of disciplinary action including suspending or terminating an employee's access to District computer resources.

### **3720.7 Vandalism**

Vandalism is defined as any purposeful attempt to harm, modify or destroy District computer software, hardware, SJECED data, or any of the other networks that are connected to the Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses. A person who commits any of the following acts not only violates this policy but may also face legal liability, including possible fines and/or imprisonment pursuant to Penal Code Section 502(c):

- 1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
- 2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
- 3) Knowingly and without permission uses or causes to be used computer services.
- 4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
- 5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.
- 6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
- 7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.
- 8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

- 9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

#### **3720.8 Access to Institutional Data**

Data users are expected to access institutional data only in their conduct of District business, to respect the confidentiality and privacy of individuals whose records they may access, to observe any ethical restrictions that apply to data to which they have access, and to abide by applicable laws or policies with respect to access, use or disclosure of information. Expressly forbidden is the disclosure of limited-access or District-internal institutional data or the distribution of such data in any medium, except as required by an employee's job responsibilities. Also forbidden is the access or use of any institutional data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy one's own personal curiosity.

#### **3720.9 Access to World-wide Data**

Faculty, staff and students will have access to the Internet, the World-Wide Web, and all related resources, from most District computers. It is intended that the Internet will be used to conduct official college business or in the pursuit of scholarship. Any restrictions on the use of the Internet by faculty, staff or students will be made either by college, departmental or office procedures.