GENERAL INSTITUTION

AP 3720 COMPUTER AND NETWORK USE

References:

Education Code Title 3. Division 7. Part 43. Sections 70901, 70902
Education Code Title 3. Division 7. Part 45. Chapter 5. Section 72400
California Code of Regulations Title 5 CCR § 58050
Penal Code Section 502
California Constitution Article 1 Section 1
Government Code Section 3543.1(b)
17 U.S. Code Sections 101 et seq.
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37 and 45
ACCJC Accreditation Standard III.C.
Reference contracts/labor agreements

The District computer and network systems are solely the property of the District. They may not be used by any person without the proper authorization of the District. The computer and network systems are primarily for District instructional and work-related purposes.

This procedure applies to all District students, faculty and staff and to others granted use of District information resources. This procedure refers to all District information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and computer communication facilities owned, leased, operated, or contracted by the District regardless of whether used for administration, research, teaching or other purposes.

Conditions of Use

Departments and Divisions within the District may define additional conditions of use for information resources under their control. These statements must be in writing and consistent with this overall procedure but may provide additional detail, guidelines and/or restrictions.

Legal Process

This procedure exists within the framework of the District Board Policy and state and federal laws. A user of District information resources who is found to have violated any of these policies may be subject to disciplinary action including but not limited to loss of

information resources privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action. Any disciplinary action will be in accordance with Board policy, negotiated labor agreements, the California Education Code, and/or Student Code of Conduct.

Copyrights and Licenses
Computer users must respect copyrights and licenses to software and other on-line information. (For copyright matters not related to software see BP/AP 3710)

- **Copying -** Software protected by copyright shall not be copied except as expressly permitted by the owner of the copyright or otherwise permitted by copyright law. Protected software shall not be copied into, from, or by any District facility or system, except pursuant to a valid license or as otherwise permitted by copyright law.

- **Number of Simultaneous Users -** The number and distribution of copies must be handled in such a way that does not violate the licensing rules of the product.

Integrity of Information Resources
Computer users must respect the integrity of computer-based information resources.

- **Modification or Removal of Equipment -** Computer users must not attempt to modify or remove computer equipment, software, or peripherals that are licensed or owned by the District, or assigned for use by others without proper authorization.

- **Unauthorized Use –** Computer users must not interfere with others' access and use of the District computers. This includes but is not limited to: unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software or computer files.

- **Unauthorized Programs -** Computer users must not intentionally:

  - develop or use programs or utilities which disrupt other computer users
  - access private or restricted portions of the District's systems
  - damage the software or hardware components of the District's systems
  - use programs or utilities that interfere with other computer uses or that modify normally protected or restricted portions of the District's systems or user accounts.

Unauthorized Access and Usage

Computer users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access.

- **Abuse of Computing Privileges -** Users of District information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the District. For example, abuse of the networks to which the District belongs or the computers at other sites connected to those networks will be treated as an abuse of District computing privileges.

- **Reporting Problems -** Any defects discovered in system accounting or system security must be reported promptly to Information Services so that steps can be taken to investigate and solve the problem.

- **Password Protection -** A computer user who has been authorized to use a password-protected account must keep their username and password secure and confidential. Users shall not share their username and password with others or use another person's username and password.

- **Usage** - Computer users must respect the rights of other computer users. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of District procedure and may violate applicable law.

- **Unlawful Messages -** Users may not use District information resources to send messages that violate applicable federal, state or other law or District policy, or which constitute the unauthorized release of confidential information.

- **Commercial Usage -** District information resources may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below). It is permissible for students to post items for sale and for the local community to post room rental notices on space provided on the Office of Student Affairs' website.

- **Information Belonging to Others -** Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, or passwords belonging to other users, without the permission of those other users.

- **Rights of Individuals -** Users must not access or release to anyone any

individual's (student, faculty, and staff) personal information stored in District information resources without proper authorization.

- **User identification -** Users shall not send communications or messages anonymously or without accurately identifying the originating account or station.

- **Political, Personal and Commercial Use Limitations -** The District is a non-profit, tax exempt organization and, as such, is subject to specific federal, state and local laws regarding sources of income, political activities, use of property and similar matters.

    1. **Political Use -** District information resources must not be used for partisan political activities where prohibited by state, federal, or other applicable laws.

    2. **Personal Use -** The computer and network systems are primarily for District instructional and work-related purposes. During work hours incidental use may be allowed and may include checking non-district email accounts, the weather, traffic, news, etc. for a brief period of time. Outside work hours, district information resources may be used for personal activities in compliance with board policies and procedures and state and federal laws. Certain computers may be designated for "public use." Examples of public use areas include designated workstations in labs or the library.

    3. **Commercial Use -** District information resources should not be used for commercial purposes or personal profit. Users also are reminded that the ".edu" domain on the Internet has rules restricting or prohibiting commercial use, and users may not conduct activities not appropriate within that domain.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of the District's network and computer resources which discriminates against any person on the basis of the categories listed in Board Policy 3410 titled 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 policy or procedure regarding discrimination or harassment.

Disclosure

- **No Expectation of Privacy –** Except as outlined in the collective bargaining

agreements with the Palomar Faculty Federation and Council of Classified Employees, the District will exercise the right to access all uses of the District telecommunications, network and computers only for legitimate District purposes, including, but not limited to, ensuring compliance with this procedure; or integrity and security of the District's systems; to address system performance issues; or to access District information when an employee is out sick or otherwise not on duty; or in response to a subpoena or court order; or when specific written permission has been granted by the Superintendent/ President. In addition, users should also be aware that Information Services, contractor or external agency personnel may have incidental access to data contained in or transported by network e-mail, voice mail, telephone and other systems in the course of routine system operation, problem resolution and support. Employees and students have no expectation of complete privacy in the use of the District telecommunications, network and computers.

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

- **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.

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

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

Title IV Information Security Compliance

In compliance with the Gramm-Leach-Bliley Act (GLBA), the District shall develop, implement, and maintain a comprehensive information security program that contains all of the following:

- A designated employee or employees to coordinate the District's information security program.

- Identification of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these

risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of the District's operations, including:

(1) Employee training and management;
(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

- Design and implementation of information safeguards to control the risks the District identifies through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

- Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
(2) Requiring the District's service providers by contract to implement and maintain such safeguards.

- Evaluate and adjust the District's information security program in light of the results of the testing and monitoring required; any material changes to the District's operations or business arrangements; or any other circumstances that the District knows or has reason to know may have a material impact on the District's information security program.

Operational Security and Data Loss Protection Training

All employees shall complete basic training in information technology operational and data security awareness, and data protection practices. This training shall be facilitated by the office of Professional Development.

Dissemination
All users shall be provided access to these procedures and directed to familiarize themselves with them.

Office of Primary Responsibility: Finance and Administrative Services