CCLC Update 36: This procedure was updated to add a section to address information security program requirements for those entities that participate in Title IV Educational Assistance Programs.

AP 3720 Computer and Network Use

Reference: ~~*Education Code Section 70902; Board Policies 3720, 4030; Title 5 Sections 58050, 58164, 58168, 58170, 58172; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45; FTC Regulations 16 CFR 313.3(n), 16 CFR 314.1-5; Gramm-Leach Bliley Act Sections 501, 505(b)(2); U.S. Code 15 USC 6801(b), 6805(b)(2)*~~ *15 U.S. Code Sections 6801 et seq.; 17 U.S. Code Sections 101 et seq.; Penal Code Section 502, Cal. Const., Art 1 Section 1; Government Code Section 3543.1(b); 16 Code of Federal Regulations Parts 314.1 et seq.; Federal Rules of Civil Procedures, Rules 16, 26, 33, 34, 37, 45; Board Policies 3720*

Date Issued: May 25, 2006 Reviewed: ~~Updated: October 21, 2014~~ ~~Updated: November 13, 2018~~

Overview

The District Computer and Network systems are the sole property of the Grossmont-Cuyamaca Community College District. They may not be used by any person without the proper authorization of the District. The Computer and Network systems are for District instructional and work related purposes only.

This procedure applies to all District students, employees, officers and 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. This includes personal computers, workstations, mainframes, minicomputers, and associated peripherals, software and information resources, regardless of whether used for administration, research, teaching or other purposes.

Conditions of Use

Basic conditions of use are also defined by the *Corporation for Education Network Initiatives in California (*CENIC)/California Research and Education Network (CalREN) Acceptable Use Policy. The District adheres to basic conditions of use and industry standards as defined by CENIC/CalREN. The District may define additional conditions of use. Refer to Operating Procedure IS 11.

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 will be subject to disciplinary action up to and 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

Nondiscrimination Statement of Principles
All users have the right to be free from any conduct connected with the use of Grossmont-Cuyamaca Community College District (GCCCD) computing systems which discriminates against any person. Discriminatory conduct includes, but is not limited to, written or graphic conduct that satisfies one of the following conditions: (1) harasses, denigrates or shows hostility or aversion toward an individual or group based on that person's gender, sexual orientation, race, color, national origin or disability, or (2) has the purpose or effect of creating a hostile, intimidating, or offensive environment. "Harassing conduct" and "hostile environment" are defined below:

- "Harassing conduct" includes, but is not limited to, the following: epithets, slurs, negative stereotyping, or threatening, intimidating, or hostile acts, that relate to race, color, national origin, gender, sexual orientation, or disability. This includes acts that purport to be "jokes" or "pranks," but that are hostile or demeaning.
- A "hostile environment" is established when harassing conduct is sufficiently severe, pervasive or persistent so as to interfere with or limit the ability of an individual to participate in or benefit from the GCCCD computing systems *(refer to Administrative Procedure AP 3410 Nondiscrimination)*.

Any user who believes he or she has been subject to a hostile environment or discrimination on the basis of race, color, national origin, gender, sexual orientation, or disability may inform the system administrator or the appropriate college or district administrator. Upon receiving any such complaint, GCCCD will process the complaint in accordance with established grievance procedures.

Academic Freedom
Users of these systems have rights that may be protected by federal, state, and local laws. This procedure shall not be interpreted in a manner which would abrogate any provision of the District Policy on Academic Freedom (Board Policy 4030).

~~**Conditions of Use**~~
~~Basic conditions of use are also defined by the *Corporation for Education Network Initiatives in California (*CENIC)/California Research and Education Network (CalREN) Acceptable Use Policy. The District adheres to basic conditions of use and industry standards as defined by CENIC/CalREN. The District may define additional conditions of use. Refer to Operating Procedure IS 11.~~

Information Security Program
The Information Security Program was created to protect District information and Personally Identifiable Information (PII) found on records and in systems owned by the District. This Program is intended as a comprehensive set of guidelines that have been implemented in compliance with regulations issued by the various controlling authorities. Refer to Information Security Program.

~~**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 will be subject to disciplinary action up to and 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.~~

Copyrights and Licenses

Computer users must respect copyrights and licenses to software and other on-line information.

- Copying – 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, 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 for the product.~~the number of simultaneous users in a department does not exceed the number of original copies purchased by that department, unless otherwise stipulated in the purchase contract.
- Copyrights – In addition to software, all other copyrighted information (text, images, icons, programs, etc.) retrieved from computer or network resources must be used in conformance with applicable copyright and other law. Copied material must be properly attributed. Plagiarism of computer information is prohibited in the same way that plagiarism of any other protected work is prohibited.

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 without proper authorization from District Information Technology.
- Unauthorized Use – Computer users must not interfere with others' access and use of the District computers. This includes but is not limited to: the sending of chain letters or excessive messages, either locally or off-campus; printing excess copies of documents, files, data, or programs, running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, of 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 (including spam, viruses and worms) which disrupt other computer users or which access private or restricted portions of the system, or which damage the software or hardware components of the system. Computer users must ensure that they do not use programs or utilities that interfere with other computer users or that modify normally protected or restricted portions of the system or user accounts. The use of any unauthorized or destructive program will result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

Unauthorized Access

Computer users must not seek to gain unauthorized access to information resources and must not assist, knowingly or unknowingly, 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 the Information Technology Department 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 may be subject to both civil and criminal liability if the user discloses the password or otherwise makes the account available to others without permission of the Information Technology Department with the exception that users may designate others to access their e-mail and voice-mail accounts.

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 electronic communication facilities to send defamatory, fraudulent, harassing, obscene, threatening, or other messages that violate applicable federal, state or other law, Student Code of Conduct or District policy, or which constitute the unauthorized release of confidential information.
- Commercial Usage – Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use, below.)
- 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. This type of information includes course-specific materials for purposes other than those intended by the instructor.
- Rights of Individuals – Users must not release any individual's (student, faculty, and staff) personal information to anyone without proper authorization.
- User Identification – Users shall not send unauthorized communications or messages anonymously or without accurately identifying the originating account or station. Examples of permissible anonymous communications are student evaluations and responses to accreditation surveys.
- Political, Personal and Commercial Use – 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. Political activities shall not include the dissemination of course-related materials discussing, presenting, or analyzing political positions, opinions or commentaries. In addition, District information technology resources must not be used for partisan political activities where prohibited by federal, state or other applicable laws, or District policies.
- Personal Use – District information resources should not be used for personal activities not related to appropriate District functions, except in a purely incidental manner. If the District otherwise grants access to the District's email system for personal use, employees may use the District's email system to engage in protected concerted activity during non-work time. Incidental uses may be allowed and may include checking non-district e-mail accounts, the weather, traffic, news, stocks, etc. for a brief period of time at the discretion of legitimate supervision. Certain computers may be designated for "public use" and non-

District functions are allowed. Examples of public use areas include specified workstations in labs, wireless hot spots, etc.

- Commercial Use – District information resources may not be used for commercial purposes. Individual personal advertisements in authorized internal newsletters will not be considered a commercial purpose. Users also are reminded that the ".cc" and ".edu" domains on the Internet have rules restricting or prohibiting commercial use, and users shall abide by the rule governing those domains.

Nondiscrimination

All users have the right to be free from any conduct connected with the use of **Grossmont-Cuyamaca Community College District** network and computer resources which discriminates against any person on the basis of **Board Policy 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.

Disclosure

- District Access to Network Computers (No expectation of Privacy) – The District ~~will exercise~~ reserves the right to monitor all use of the ~~access all uses of the~~ District network and computers to assure ~~only for legitimate District purposes, including, but not limited to, ensuring~~ compliance with this procedure.~~; or integrity and security of the system; 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.~~ In addition, users should also be aware that Information Technology, 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~~Users should be aware that they have no expectation of privacy in the use of the District network and computers resources. The District will exercise this right only for the legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system, access District information when an employee is out sick or otherwise not on duty; or in response to a subpoena or court order.
- ~~Possibility of Unintended Disclosure~~ – Users must be aware of the possibility of unintended disclosure of communications.
- District's Disclosure Responsibility – Users must be aware that all electronic communications and electronic documents may be subject to disclosure by the District in response to law enforcement investigations, judicial orders, California Public Records Act requests and other requests/demands that are outside of the District's control to limit or deny. Additionally, the District may be prohibited from notifying the user of the disclosure demand and/or the response to that demand.
- 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 computers must be disclosed by the District if requested by a member of the public.

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

Dissemination and User Acknowledgment of this Procedure
All users shall be provided copies of these procedures and be directed to familiarize themselves with them.

Any disciplinary action will be in accordance with Board policy, labor/management negotiated agreements, and the *Student Discipline Procedures* handbook.

A "pop-up" screen addressing the e-mail portions of these procedures shall be installed on all e-mail systems. The "pop-up" screen shall appear prior to accessing the e-mail network. Users shall sign and date an acknowledgement and waiver included in this procedure stating that they have read and understand this procedure, and will comply with it. ~~Where possible, a "pop-up" screen describing the agreement shall appear prior to accessing the network.~~

This acknowledgment and waiver shall be in the form as follows:

Acknowledgment

Computer and Network Use Agreement

I have received and read a copy of the District Computer and Network Use Procedures and this Agreement dated, _____, and recognize and understand the AP 3720 guidelines. I agree to abide by the standards set in the Procedure for the duration of my employment and/or enrollment. I am aware that violations of this Computer and Network Usage Procedure may subject me to disciplinary action, including but not limited to revocation of my network account up to and including prosecution for violation of State and/or Federal law.

_____ _____
Print Name Date

_____
Signature

Note: This page will be kept and filed by originating department.

Title IV Information Security Compliance

NOTE: *This section is **suggested as good practice** for those entities that participate in Title IV Educational Assistance Programs. The Gramm-Leach-Bliley Act requires entities that participate in Title IV Educational Assistance Programs to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the entity's size and complexity, the nature and scope of the entity's activities, and the sensitivity of any customer information at issue. If an entity does not insert its locally developed information security program here, it should ensure it is maintained elsewhere in writing and meets the requirements of the Act. The Act requires an information security program contain all of the following:*

- A designated employee or employees to coordinate the entity'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 entity'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 entity 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 entity's service providers by contract to implement and maintain such safeguards.

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