ADMINISTRATIVE PROCEDURE 3720 TELEPHONE, COMPUTER AND NETWORK USE

The Chancellor directs that the following regulations and procedures apply to all Peralta Community College District students, faculty, staff, administrators, consultants, authorized guests, and to any other persons granted use of District information resources. The District is responsible for making these procedures and policies readily accessible to all users prior to their use of the District Network (See Section II. C., as an example). These regulations and procedures refer to all District Network resources whether individually controlled or shared, stand-alone or networked. It applies to all telephone and communication systems, computer and computer communication facilities owned, leased, operated, or contracted by the District. This includes, but is not limited to, telephones, personal computers, laptops, workstations, tablets, servers, network devices, mobile devices, and associated peripherals, printers, fax machines, software and information resources, regardless of whether used for administration, research, teaching or other purposes. Hereinafter, this system and all of its components shall be referred to as the "District Network."

I. Legal Parameters. Abuse of computing, networking, or information resources contained in or part of the District Network may result in the loss of access to the District Network. Additionally, abuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable District or college policies, procedures, State and Federal laws, 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.

A. **Property**. The District Network systems are the sole property of the Peralta Community College District ("District"). They may not be used by any person without the proper authorization of the District. Except as provided in Board Policy, collective bargaining agreements, or as pursuant to Federal or State law 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.

B. **Regulations.** This administrative procedure exists within the framework of the District Board Policy and state and federal laws. A user of District Network resources who is found to have violated any of this administrative procedure's regulations will be subject to disciplinary action up to and including but not limited to loss of District Network privileges; disciplinary suspension or termination from employment or expulsion; and/or civil or criminal legal action.

1. **Copyrights and Licenses.** Computer users must respect copyrights and licenses to software and other on-line information. 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.
2. **Copying.** Software protected by copyright may not be copied or published, 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, as it pertains to "fair use" guidelines.
3. **Network Usage.** Downloading, uploading, file sharing, copying, or publishing unlicensed or copyrighted movies, music, and "codes" for other than legally authorized uses or uses authorized by the District is prohibited.
4. **Number of Simultaneous Users.** The number and distribution of software copies must be handled in such a way that 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.
5. **Removal of Equipment.** Computer users must not attempt to and/or remove telephones, computer equipment, software, or peripherals without management authorization (expressed or

implied), this includes, but is not limited to, District purchased and/or owned personal computers, laptops, tablets, mobile devices, etc.

II. Unauthorized Computer and Network Use

A. **Interference with Access.** Computer users must not interfere with others access and use of the District Network. This includes, but is not limited to, excessive email messages, running and/or installing grossly inefficient programs when efficient alternatives are known by the user to be available; excessive printing of documents, files, data, or programs; unauthorized modification of system facilities, operating systems, or network storage devices; attempting to crash or tie up a District computer or network; and damaging or vandalizing District computing facilities, equipment, software or computer files.

B. **Disruptive Programs.** Computer users must not intentionally develop or use programs 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 intentionally 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 may result in disciplinary action as provided in this procedure, and may further lead to civil or criminal legal proceedings.

C. **Abuse of Computing Privileges.** Users of District Network resources must not knowingly 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. Additional examples of behaviors constituting abuse which violate this Board Policy include, but are not limited to, the following activities:
    a. Using a computer account that one is not designated or authorized to use.
    b. Obtaining a password for a computer account that one is not authorized to have and/or knowingly or carelessly allowing someone else to use your account.
    c. Using the District Network to gain unauthorized access to any computer systems.
    d. Knowingly performing an act which will interfere with the normal operation of the District network resources.
    e. Knowingly running or installing on the District Network, a program intended to take control of the District Network resources, or giving another user, a program intended to damage or to place excessive load on the District Network. This includes, but I not limited to programs known as malware: computer viruses, Trojan horses, zombie software and worms.
    f. Masking the identity of an account or machine or forging e-mail messages.
    g. Attempting to circumvent data protection schemes or uncover or exploit security and/or loopholes.
    h. Deliberately wasting District Network resources by file sharing schemes, participating in e-mail chains, spamming, and/or excessive bandwidth usage.
    i. Attempting and/or accessing, without District authorization to monitor or tamper with another user's electronic communications, or changing, or deleting another user's files or software without the explicit agreement of the owner, or any activity which is illegal under California computer Crime Laws.
    j. Using the District Network for gambling purposes.
    k. Use of District Network for political purposes shall be subject to state and federal law and Board of Trustees approval where the law is permissive.

D. **Unlawful and Prohibited 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 or District policy, or which constitute the unauthorized release of confidential information. The sending of chain letters or excessive messages, either locally or off campus is also prohibited.

1. **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 users.
2. **Rights of Individuals.** Users must not release any individual's (student, faculty, and staff) personal information to anyone without proper authorization. However, both the nature of electronic communication and the public character of District business make electronic communication less private than many users anticipate, and may be subject to public disclosure.
3. **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.
4. **Political Use.** District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.
5. **Commercial Usage.** District electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions. Commercial use means for financial remuneration or designed to lead to financial remuneration.

E. **Prohibited Activities**

1. **Personal Use.** District Network resources should not be used for activities not related to appropriate District functions. Although personal use is not an intended use, the district recognizes that the network will be used for incidental personal activities provided that such use is within reason and provided that such usage is ordinarily on an employee's own time, is occasional at most, and does not interfere with or burden the District's operation, and not otherwise contrary to District Policies, Procedures, or law.
2. **Commercial Use.** District information resources are not to be used for any commercial purposes. Users are reminded that the District's license for the ".cc" and ".edu" domains on the Internet prohibits commercial use, and users may not conduct commercial activities with those domains.
3. **Harassment.** Using District Network resources to harass others is explicitly prohibited and can be subject to legal ramifications. Examples of such activity include, but are not limited to, the use of the District Network to:
    a. Threaten others via telephone, email, voicemail, or text.
    b. Publish defamatory information about another person.
    c. Knowingly downloading, displaying or transmitting communications, images, drawings, depictions that contain sexually explicit materials, ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on race, national origin, sex, sexual orientation, age, disability, religious or political belief as it pertains to District discrimination and harassment policies, as well as State and Federal regulations.

III. **District Users Rights and Responsibilities.** This Procedure applies to all members of the Peralta Community College District community utilizing the District Network. The Procedure covers the use of all District software, technology systems, computer equipment, and communications systems throughout PCCD. If any provision of this procedure is found to be legally invalid it shall not affect the other provisions of the procedure.

A. **Ownership Rights.** This procedure is based upon and shall be interpreted according to the following fundamental principle: the entire District Network, and all hardware and software components with it, is the sole property of the District which sets the terms and conditions of its use consistent with the law. 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.

B. **District Rights.** System administrators may access user files or suspend services they manage without notice only during one or more of the following occurrences:

a. To protect the integrity and/or security of the District Network resources
b. Under time-dependent, critical operational circumstances
c. As required by and consistent with the law
d. Where evidence exist that violations of the law or District Policy or Procedures have occurred

For example: System administrators, following organizational guidelines, may access or examine individual files or accounts based on evidence that they have been corrupted or damaged or subject to unauthorized use or misuse. In such cases, without notice, data or information acquired may be used to initiate or extend an investigation related to the initial cause or as required by law or Board Policy and/or to protect system integrity. This may or may not include personal electronic storage owned by or under control of individuals including cloud storage.

C. **User Rights.** While the District monitors electronic usage as part of its normal network operating procedures, the District does not routinely inspect or monitor users' computer hardware or files, email, and/or telephone message system, nor disclose information created or stored in such media without the user's consent. The District shall attempt to notify users before accessing computer hardware and files or prior to suspending service. In the event that the District acts without consent, it shall notify the user as soon as possible of its access and provide the reason for its action.

D. **User Responsibilities.** The District recognizes that computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users; respect the integrity of the systems and related physical resources and observe all relevant law, regulations, and contractual obligations.

The interaction of a user's personal computing equipment, connected to the District Network, is subject to the procedures in this document. Contents of a user's personal computing equipment are subject to search by the District only by reasonable means.

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 herein and within the *District Acceptable Computer Use* Guidelines.

IV. Disclosure

A. **Privacy Interests.** The District recognizes the privacy interests of its employees and students and their rights to freedom of speech, shared governance, and academic freedom, as well as their right to engage in protected union and concerted activity. The District reserves the right to monitor all use of the District Network and resources to assure compliance with these policies. The District will exercise this right only for legitimate District purposes; including but not limited to court ordered discovery proceedings, freedom of information act disclosures, and ensuring compliance with this procedure and the integrity and security of the system, etc. The District seeks to afford email communications privacy protections comparable to those it traditionally affords paper mail and fax communications, consistent with State and Federal statutes.

B. **Possibility of Disclosure.** Users must be aware of the possibility of unintended disclosure of communications. The District Network can be subject to authorized and unauthorized access by both

internal and external users. There are virtually no online activities or services that guarantee an absolute right of privacy, and therefore the District Network is not to be relied upon as completely confidential and private.

C. **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.

D. **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 if requested by a member of the public.

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

F. **Dissemination and User Acknowledgement.** All users of the District Network must comply with Board Policy, as well as this Administrative Procedure 3720, and any additional guidelines established by the District. Such guidelines will be reviewed by the District and may become subject to Board approval as a District policy or procedure. All users shall be provided copies of these regulations, procedures, and guidelines; be directed to familiarize themselves with them, and agree to terms of usage. By using any part of the District Network, users agree that they will comply with the Policy and Procedures.

1. **Procedure.** A process addressing these procedures shall be installed. The process shall appear prior to accessing the secured system. Users shall sign and date the acknowledgement and waiver included in this procedure stating that they have read and understand this procedure, and will comply with it and its associated regulations. This acknowledgment and shall be in the form as follows:

2. **Computer and Network Use Agreement.** I have received and read a copy of the District Telephone, Computer, and Network Use Procedures and this Agreement dated February 19, 2013. I recognize and understand the guidelines. I agree to abide by the standards set the in the Procedures for the duration of my employment and/or enrollment. I am aware that violations of this Telephone, 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.

V. 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.

2. 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:

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

3. 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.

4. Oversee service providers, by:
(a) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
(b) Requiring the 3. entity's service providers by contract to implement and maintain such safeguards.

5.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.

References:

15 U.S. Code Section 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 Procedure, Rules 16, 26, 33, 34, 37, 45
California Community Colleges Technology Center Security Standard
http://cccsecuritycenter.org/downloads/category/1

Approved by the Chancellor: February 19, 2013
Revised and approved by the Chancellor: August 7, 2014
Revised and approved by the Chancellor: January 5, 2021