Coast Community College District
Administrative Procedure
Chapter 3
General Institution

AP 3720 Computer and Network Use

References:

Education Code Section 7054;
17 U.S. Code Sections 101 et seq;
18 U.S. Code Section 2520 ;
Penal Code Section 502, Cal. Const., Art. 1 Section 1;
Government Code Section 3543.1(b);
Government Code Section 8314;
California Civil Code 1798.29(g);
BP/AP 3710 Securing of Copyright;
BP/AP 3750 Use of Copyrighted Material;
BP/AP 3410 Prohibition of Unlawful Discrimination, and Harassment, and Retaliation

This Procedure applies to all members of the District community using the District Network including, but not limited to, faculty, administrators, staff, students, independent contractors, and authorized guests. The Procedure covers the use of all District computer equipment and communication systems in computer labs, classrooms, offices, and libraries, and the use of the District equipment, servers, systems, and networks from any location. If any provision of this Procedure is found to be legally invalid, it shall not affect the other provisions of this Procedure as long as they can be effective without the invalid provision.

Ownership Rights
This Procedure is based upon and shall be interpreted according to the following fundamental principle: the entire District Network, including 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 Policies, Administrative Procedures, and collective bargaining agreements pertaining to intellectual property rights, network users 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.

Privacy Interests
The District recognizes the privacy interests of faculty and staff and their rights to freedom of speech, participatory governance, and academic freedom, 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 the District's business make electronic communication less private than many users anticipate, and may be subject to public disclosure. In addition, the District Network can be subject to authorized and unauthorized access by both internal and external users. For these reasons, there are no online activities or services that guarantee an absolute right of privacy, and therefore, the District Network is not to be relied upon as confidential or private. Nonetheless, 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 laws. The District will also provide voice mail protection to the extent required by the Federal Wiretap Act.

District's Rights

System administrators may access user files or suspend service that they manage without notice only: (1) to protect the integrity of computer systems; (2) under time-dependent, critical operational circumstances; (3) as required by and consistent with the law; or (4) where evidence exists that violations of law or Board Policies or Administrative Procedures have occurred. For example, system administrators, following District 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 of access 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 or Administrative Procedure and/or to protect system integrity.

Access to any aspect of the District enterprise resource planning ("ERP") system or other District applications containing personally identifiable information ("PII") or protected health information ("PHI"), or any other student or employee information protected by state or federal law, shall be granted upon the successful completion of the Department of Justice ("DOJ") Live Scan fingerprint check.

In order to ensure effective handling of emergency situations, the District monitors calls only when an emergency call is made to 911. Call monitoring will not be available during any other call regardless of number or extension dialed. Emergency calls can only be monitored by Campus Safety director and officers. Campus Safety cannot be heard during monitoring; they can only listen. 911 monitoring allows Campus Safety to be aware of the emergency situation so they can better communicate and assist campus personnel, Police, Fire, and other emergency responders.

User Rights

The District utilizes automated processes to monitor electronic usage as part of its normal network operating procedures. The District shall attempt to notify users before authorized personnel access computer hardware and files or prior to suspending service. In the event that the District acts without user consent, under its District's Rights specified above, the District shall do so with the least perusal of contents and the least action necessary to resolve the immediate situation. When the District accesses files without user consent, it shall notify the user as soon as practical of its access and provide the reason for its action.

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 laws, regulations, policies, procedures, and contractual obligations.

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 or other authorized activities.

Although personal use is not an intended use, the District recognizes that the District 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, and does not

interfere with or burden the District's operation, and is not otherwise contrary to Board Policies or Administrative Procedures.

"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. In addition, no Personally Identifiable Information (PII) unrelated to District matters should be stored or transmitted using the District Network.

All users of the District Network must read, understand, and comply with this Procedure as well as any additional guidelines established by the District. Such guidelines will be reviewed by the District and may become subject to Board approval as a Board Policy or Administrative Procedure. By using any part of the District Network, users agree that they will comply with this Procedure.

Enforcement of the Procedure

The Chancellor or designee will enforce applicable federal and state laws, Board Policies and Administrative Procedures, including not only those laws and regulations that are specific to computers and networks but also those that apply generally to personal conduct. Violations of this Procedure will be dealt with in the same manner as violations of other Board Policies or Administrative Procedures or standards of behavior and may result in disciplinary action, subject to applicable due process requirements. Such violations may be subject to appropriate personnel action and/or criminal investigation.

Users who believe this Procedure has been misinterpreted or misapplied may file a complaint in accordance with the Complaint Procedures noted below.

Students who do not observe the requirements of this Procedure may be in violation of the Student Code of Conduct and subject to student discipline. Employees who do not observe the requirements of this Procedure may be subject to disciplinary action up to and including termination.

This Administrative Procedure shall be distributed to all new and existing employees. Nothing in this Procedure should be construed to interfere with First Amendment rights or with the academic freedom of faculty.

The District is responsible for making this Procedure readily accessible to all users prior to their use of the District Network. 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 laws. Users may be held accountable for their conduct under any applicable Board Policies, Administrative 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.

System Abuse

Examples of system abuse include, but are not limited to, the following:

• Using a computer account that one is not authorized to use.

• Obtaining a password for a computer or application or system account that one is not authorized to have.
• Using the District Network to gain unauthorized access to any information technology systems.
• Knowingly performing an act which will interfere with the normal operation of applications, systems, computers, terminals, peripherals, or networks.
• Knowingly running or installing on any system or network - a program intended to take control of the computer(s) or systems, or giving to another user - a program intended to damage or to place excessive load on a system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, zombie software, and worms.
• Knowingly or carelessly allowing someone else to use an account.
• Forging e-mail messages.
• Attempting to circumvent data protection schemes or uncover or exploit security loopholes.
• Masking the identity of an account or machine.
• Deliberately wasting computing resources by file sharing schemes, participating in e-mail chains, spamming, and/or excessive bandwidth usage.
• Intentionally accessing, downloading, displaying, uploading, or transmitting obscenity, as legally defined.
• Attempting 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 permission of the owner, or any activity which is illegal.
• Personal use which is excessive or which interferes with the user's or others' performance of job duties, or otherwise burdens the intended use of the Network.
• Using the District Network for online gambling.
• Using the District Network for political purposes as set forth in Education Code Section 7054.

Harassment

• Using the District Network, including telephone, e-mail, or voice mail, to harass or threaten others.
• Knowingly downloading, displaying, or transmitting by use of the District Network, communications, pictures, drawings or depictions that that do not constitute proper exercise of academic freedom or constitutionally protected free speech or expression.
• Knowingly downloading, displaying, or transmitting by use of the District Network sexually explicit images, messages, pictures, or cartoons which have the clear purpose of harassment or have been identified as harassment as the result of a formal investigation into the matter.
• Knowingly downloading, displaying, or transmitting by use of the District Network sexually harassing images or text that do not constitute proper exercise of academic freedom or constitutionally protected free speech or expression which in a public computer facility, or location that can potentially be in view of other individuals.
• Using the District Network to publish defamatory information about another person.

Commercial use

• Using the District Network for any commercial activity, other than incidental or traditional commercial use, without written authorization from the District. "Commercial activity" means for financial remuneration or designed to lead to financial remuneration. Examples of "incidental or traditional commercial use" include but are not limited to:

- Electronic communication between an instructor who is an author of a textbook and her/his publisher.
- Electronic communication by a staff member who uses the District Network to communicate regarding a presentation at an educational conference or workshop for which that staff member might receive an honorarium.
- Electronic use by a student of the District Network to seek a part-time or full-time job or

career related to the student's field of study, or to assist her/him in applying for such work.
- Electronic communication by a staff member to inform a colleague about their child's candy bar fundraising sale for the child's school.
- Using electronic resources to research and/or purchase supplies, equipment, or other items required for campus, District, or student use.

Copyright

- Violating terms of applicable software licensing agreements or copyright laws.
- Publishing copyrighted material without the consent of the owner on District websites in violation of copyright laws.
- Downloading of unlicensed or copyrighted movies or music for other than legally authorized uses or uses authorized by the District.
- Illegally downloading copyrighted material or information that would enable the unauthorized utilization of copyrighted material.

Exceptions

The interaction of a user's personal computing equipment, connected to the District Network, is subject to this Procedure. Contents of a user's personal computing equipment are subject to search by the District only by legal warrant.

There may be times when District employees may be exempted from certain provisions of this Procedure in order to perform their duties or assignments that are an established part of their job.

Should an employee be directed by a supervisor to perform an activity that they believe may be in violation of this Procedure, or if they are given a directive which inhibits the employee in performing his/her duties or assignments, the employee may request that the directive and/or permission for exception be put in writing and signed by the supervisor.

Activities by technical staff as authorized by appropriate District or college officials that 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 resources. Likewise, the District will not purposefully surveil or punish use of the network for union business-related communication between employees and their unions.

Complaints by Employees or Students Regarding Enforcement of this Procedure

An employee who asserts that the District or District personnel have violated this Procedure may file a complaint using the "Report An Issue" online form posted on the District web site under the Internal Audit department or by contacting the District Director Internal Audit. A student who asserts that the District or District personnel have violated this Procedure may file a complaint pursuant to the College's student complaint process.

Ratified March 21, 2018
Ratified December 12, 2018
Ratified February 3, 2021