Coast Community College District
BOARD POLICY
Chapter 5
Personnel Policies and Human Resources

BP 3720 Computer and Electronic Resources Systems Acceptable Use Policy

The Coast Community College District ("District") owns, leases, and/or operates a variety of computer and communication systems, including but not limited to, voicemail, electronic mail (e-mail), telephone, and access to the internet, which are provided for the use of District faculty, administrators, staff, and students in support of the programs of the colleges and District. Hereinafter, this system and all of its component parts shall be referred to as the "District Network." This network establishes a communications platform that often substitutes for in-person meetings regarding District business.

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

Ownership Rights

This Policy 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.

Privacy Interests

The District recognizes the privacy interests of faculty and staff and their rights to freedom of speech, shared 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 District 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 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 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 statutes. The District will also provide voice mail protection to the extent required by the Federal Wiretap Act.

District Rights

System administrators may access user files or suspend services 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 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 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 and/or to protect system integrity.

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 user consent, under its District 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 possible of its access and provide the reason for its action.

User Responsibilities

The Board 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.

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.

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, and does not interfere with or burden the District's operation, and not otherwise contrary to District policies or 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. These types of prohibited uses and purposes are further defined in the attached Administrative Procedures.

All users of the District Network must read, understand, and comply with this Policy as well as the accompanying Administrative Procedures, 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. By using any part of the District Network, users agree that they will comply with this Policy.

Enforcement of the Policy

The Board directs the Chancellor or designee to enforce all existing federal and state laws and District and college policies, 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 Policy will be dealt with in the same manner as violations of other District policies 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 policy has been misinterpreted or misapplied may file a complaint in accordance with the Complaint Procedures found in the accompanying Administrative Procedures.

Students who do not observe the requirements of this Policy may be in violation of the Student Code of Conduct and subject to student discipline.

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

COMPUTER AND ELECTRONIC RESOURCES SYSTEMS ACCEPTABLE USE PROCEDURE

The District is responsible for making these procedures and the policy that they implement 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 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.

District employees and students accused of violating this Board Policy have the right to representation. Absent a negotiated agreement to the contrary, State statutes will apply.

Examples of behaviors constituting abuse which violate this Board Policy include, but are not limited to, the following activities:

System abuse

- Using a computer account that one is not authorized to use.
- Obtaining a password for a computer account that one is not authorized to have.
- Using the District Network to gain unauthorized access to any computer systems.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals or networks.
- Knowingly running or installing on any computer system or network, a program intended to take control of the computer(s), or giving to another user, a program intended to damage or to place excessive load on a computer 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 your account who engages in any misuse in violation of the accompanying Board Policy.
• Forging e-mail messages and/or forwarding email specifically marked as confidential.
• 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 or pornography 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 agreement of the owner, or any activity which is illegal under California Computer Crime Laws.
• Personal use which is excessive or 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 shall be subject to state and federal law and Board of Trustees approval where the law is permissive.

Harassment

• Using the 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 contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political belief.
• 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 in a public computer facility, or location that can potentially be in view of other individuals.
• Using the District Network to publish false or 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 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 his/her 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 Web sites 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 the "codes" to copyrighted material even if the software in question is not downloaded.

Exceptions

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 legal warrant.

There may be times when a District employee may be exempted from certain provisions of these procedures 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 they believe may be in violation of this policy, 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 Bargaining Unit Employees or Students Regarding Enforcement of the Electronic Use Policy

A bargaining unit employee who asserts that the District or District personnel have violated this policy may file a grievance per that user's current collective bargaining agreement. A student who asserts that the District or District personnel have violated this policy may file a grievance per his/her college's student grievance procedure.

Adopted January 19, 2005
Revised February 20, 2008
Replaces CCCD Policy 050-1-6.2, Spring 2011