

ACCEPTABLE TECHNOLOGY USE

The District technology systems are the sole property of Contra Costa Community College District. They may not be used by any person without the proper authorization of the District. The technology systems are for District instructional and work related purposes only.

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. 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.

1. Conditions of Use

Computer Technology users shall only use the designated accounts as assigned and authorized by the District. Users **are required to shall** keep all IDs, passwords, and personal account information confidential and **shall** take reasonable precautions to prevent others from obtaining this information. **This includes staying informed about common phishing tactics by completing required training and actively taking steps to reduce the likelihood of becoming a victim.** Accounts are not transferrable and users shall not share their credentials or allow others to have access to their account. **Except in the case of a verified breach, each user is will** responsible for any use of activity conducted through their accounts, including actions by others to whom **they have granted access. has been given.**

2. Legal Process

This procedure exists within the framework of 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, **or and** civil or criminal legal action.

3. Copyrights and Licenses

Computer users must respect copyrights and licenses to software and other online information.

3.1 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.

3.2 Number of Simultaneous Users

The number and distribution of 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.

3.3 Copyrights

Computer Technology users are responsible for using software and electronic materials in accordance with copyright and licensing restrictions. **Computer uUsers are required shall** to abide by all applicable copyright and trademark laws and to abide by all licensing agreements and restrictions. **Computer uUsers** shall not copy, transfer or utilize any software or electronic materials in violation of such copyright, trademark, and/or licensing agreements. The copying of software that has not been placed in the public domain and distributed as "freeware" is expressly prohibited by this procedure. Users who access, copy, transfer, and/or use "shareware" are expected to abide by the requirements of the

shareware licensing agreement. No user may inspect, change, alter, copy, or distribute proprietary data, programs, files, disks, or software without proper authority.

4. Integrity of Information Resources

Computer Technology users shall not attempt to modify any system or network or attempt to crash or hack into District systems or any other systems. **Computer Users** shall not tamper with any software protections or restrictions placed on computer applications or files. Unless properly authorized, **computer** users shall not attempt to access restricted portions of any operating system or security software. **Computer Users** shall not attempt to remove existing software or add their own personal software to District computers and systems unless properly authorized. **Computer Users** must respect the integrity of computer-based information resources.

4.1 Modification or Removal of Equipment

Computer Technology users must not attempt to modify or remove computer equipment, software, or peripherals that are owned by others without proper authorization.

4.2 Unauthorized Use

Computer Technology 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 **the user knows** efficient alternatives ~~are known by the user~~ to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a District computer or network; damaging or vandalizing District computing facilities, equipment, software or computer files; ignoring or disobeying policies and procedures established for specific computer labs; surfing inappropriate websites such as those that are sexually explicit, gambling related, or that subscribe to hate propaganda; and/or knowingly or carelessly introducing any invasive or destructive programs (i.e. viruses, worms, Trojan Horses) into District computers or networks.

5. Unauthorized Access

Computer Technology users must not seek to gain unauthorized access to information resources and must not assist any other persons to gain unauthorized access. Computer users must not use another user's credentials (ID/password) to access information resources.

5.1 Abuse of Computing Privileges

Computer Technology 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.

5.2 Reporting Problems

~~Any~~ All cybersecurity threats, defects discovered in system accounting, or system security vulnerabilities, suspected phishing attempts, and social engineering attacks must be reported promptly to the District Information Technology department so steps can be taken to investigate and resolve the **problem issue**.

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.

6. Usage

Computer Technology 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~~ and conduct themselves with professionalism and civility. The use of District technology resources must align with all applicable District policies and reflect the ethical standards outlined in Human

Resources Procedure 1040.08 – Employee Code of Ethical Behavior and Student Services Procedure 3027 – Standards of Student Conduct.

Any attempt to bypass security measures to gain unauthorized access to systems, accounts, or another person's information is a violation of District procedures and may also constitute a violation of applicable laws.

6.1 Email and Digital Communication Unlawful Messages

Users should be aware that email is a permanent and potentially public form of communication and should not be used with any expectation of privacy.

Users must observe the following guidelines when using District email and digital communication systems:

- Use District email only for work-related activities.
- Use blind carbon copy (BCC) when sending messages to large groups to prevent recipients from replying to all other recipients simultaneously. All emails sent to college and/or district distribution lists must be sent using BCC only. Senders must include the names of the BCC'd distribution list(s) at the bottom of emails so recipients are aware of which groups received the message.
- All Employee distribution lists are intended for sharing general college or District information, not as forums for discussion or for sharing articles, social-media posts, or similar content not directly connected to college or District activities. Content must be of broad interest to all recipients. Messages containing personal opinions or information not relevant to the entire group should not be sent using group lists.
- Emails to All Employee distribution groups are subject to moderation and approval prior to distribution. These lists should only be used for work-related, general announcements that support the District's educational mission. Appropriate topics include:
 - College or District operational updates or planning activities
 - Events or initiatives that enhance the student educational experience
 - Employee professional development opportunities
 - Emergency alerts or notifications
 - Information about internal career opportunities or employee benefits
 - Announcements and updates from constituency group leaders
- Never attach, link to, or otherwise include any content that would violate District policies or state or federal law.
- Use District email in compliance with the security protocols outlined in Business Procedure 22.22 – Data Classification Standard. Do not use email to send personally identifiable, confidential, or otherwise protected information about any individual or group.

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.

6.2 Commercial Usage

~~Electronic communication facilities may not be used to transmit commercial or personal advertisements, solicitations or promotions (see Commercial Use below).~~

6.3 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.

6.4 Rights of Individuals

Users must not release any individual's (student, faculty, or staff) personal information to anyone without proper authorization.

6.5 User Identification

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

6.6 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.

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

District information resources should not be used for personal activities not related to 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.

District information resources should not be used for commercial purposes, including but not limited to sending advertisements, solicitations, or promotions to advance or support external for-profit or revenue-generating activities, events, or services. Users also are reminded that the ".edu" domain, on the internet as well as the District's internet service provider (CENIC), has rules restricting or prohibiting commercial use, and users may not conduct activities not authorized within that domain.

7. Nondiscrimination

All users have the right to be free from any conduct connected with the use of District technology resources which discriminates against any person on the basis of Board Policy 2001. No user shall use District technology 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.

8. Disclosure

8.1 No Expectation of Privacy

The District reserves the right to monitor all use of technology to assure compliance with applicable policies and procedures. Users should be aware that they have no expectation of privacy in the use of technology. The District will exercise this right only for legitimate District purposes, including, but not limited to, ensuring compliance with this procedure and the integrity and security of the system. The contents of files and electronic messages stored in the District network may be viewed by a system administrator in the course of routine maintenance or as needed for District administrative purposes, including investigation of possible violations of this or any other procedure.

8.2 Possibility of Disclosure

Users must be aware of the possibility of unintended disclosure of communications.

8.3 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.

8.4 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 or computers must be disclosed if requested by a member of the public.

8.5 Litigation

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

9. Ethical Standards

The Contra Costa Community College District's technology resources offer powerful tools for open learning and exchange of ideas. If this electronic medium of exchange is to function well and support an open, caring community of learners, its users need to agree to and abide by ethical standards of online behavior that assure all users full, equitable, effective, and efficient access and use. Such ethical standards include but are not limited to:

9.1 Honesty

Users agree to represent themselves according to their true and accurate identities in all electronic messages, files, and transactions at all times. ~~While~~When using technology resources, users agree to ~~behave within~~ **adhere to** the standards described in applicable college or District policies, procedures, or collective bargaining agreements.

9.2 Students and Employees

In using the District's technology resources, users must communicate in the same manner as is expected in the classroom or on campus. The distance provided by electronic communications does not create a forum in which there are no ethical or legal limitations. Users shall not use District technology resources in any unlawful manner including, but not limited to, attempting to defraud another, threatening physical harm to another, procuring or distributing obscene material in any form, or unlawfully harassing another.

While the District recognizes and respects users' rights to freedom of speech, such rights are not absolute. Speech ~~that~~which is fraudulent, libelous, obscene, harassing, or threatening is not permitted under state or federal law. Users are expressly prohibited from using the District's technology resources to engage in such conduct. Users violating this section will be subject to revocation of their user accounts and District technology resources.

For purposes of this procedure, the terms fraud and libel are given their legal meaning as developed by the courts of this State and of the United States. "Obscenity" means words, images or sounds which a reasonable person, applying contemporary community standards, when considering the contents as a whole, would conclude that they appeal to prurient sexual/physical interests or violently subordinating behavior rather than an intellectual or communicative purpose, and materials that, taken as a whole regarding their content and their particular usage or application, lack any redeeming literary, scientific, political, artistic or social value. "Threatening" means communications which result in an individual being fearful of imminent bodily harm and/or emotional/mental disruption of ~~their~~ **his/her** daily life. "Harassing" means to engage in a knowing and willful course of conduct directed at another ~~that~~which seriously alarms, annoys, or harasses another, and which serves no legitimate purpose. In addition, "harassment" shall also mean to subject another to unwelcome sexual advances, requests for sexual favors, and other verbal, visual, or physical conduct of a sexual nature as set forth in California Education Code Section 212.5.