CITRUS COMMUNITY COLLEGE DISTRICT
GENERAL INSTITUTION

AP 3720 ACCEPTABLE COMPUTER AND NETWORK USE

References: Education Code Section 70902; 17 U.S.C. Section 101 et seq.; Penal Code Section 502, Cal. Const., Art. 1 Section 1; Government Code Section 3543.1(b); Family Educational Rights and Privacy Act of 1974; Gramm-Leach-Bliley Act (GLBA). ACCJC Accreditation Standard 3.2, 3.9 & 3.10; 15 U.S. Code Sections 6801 et seq; 17 U.S. Code Sections 101 et seq.; 1 Code of Federal Regulations Parts 314.1 et seq.; Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

Purpose

In support of its mission, Citrus Community College District provides computing facilities, networking, and information technology resources for use by all individuals, including but not limited to faculty and visiting faculty, staff, students, alumni, the Board of Trustees, visitors, or external individuals and organizations. The District encourages the use of its computing facilities to manage and share information, to improve communication, and to develop and exchange ideas.

Scope

This procedure applies to all users of computing resources owned or managed by the District. Individuals covered by the policy include (but are not limited to) faculty and visiting faculty, staff, students, alumni, the Board of Trustees, guests or external individuals and organizations accessing network services via the District's computing facilities.

Computing resources include all District owned, licensed, or managed hardware, software, and websites that use the District network via a physical or wireless connection, regardless of the ownership of the computer or device connected to the network. This procedure applies to technology administered in individual departments, resources administered by central administrative departments, personally owned computers and devices connected by wire or wireless to the District network, and off-District computers that connect remotely to the District's network services.

Procedures

User Rights and Responsibilities

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 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, and contractual obligations.

Those that use District computing resources are expected to do so responsibly and to comply with state and federal laws and regulations, and District policies and administrative procedures. In all instances, users are expected to comply with the District's Institutional Code of Ethics and the Students Standard of Conduct.

Users of District systems have the responsibility to:

- Use the systems in compliance with the procedures presented.
- Comply with all applicable laws.
- Access systems only as authorized.
- Keep passwords secret and maintain password and account security.
- Prevent use of their account by others.
- Use the system with proper etiquette and respect for other users.
- Refrain from acts that are discriminatory, defamatory, harassing, or illegal.
- Report perceived vulnerabilities to the District's services or hosted applications.

Acceptable Use

Acceptable use means respecting the rights of other computer users, the integrity of the physical facilities, and all related license and contractual agreements. The application of this principle to District computing resources includes the following for each user:

- Use only the computers, computer accounts, and computer files for which authorization has been provided. Do not use another individual's account or attempt to capture or guess other users' passwords.
- Be responsible for appropriate use of all resources assigned including the computer, the network address or port, software, and hardware.
- Guard against unauthorized users access to the network by using a District computer or a personal computer that is connected to the District network.
- Comply with all such agreements when using such resources, as the District is bound by its contractual and license agreements respecting certain third-party resources.
- Make a reasonable effort to protect passwords and to secure resources against unauthorized use or access.
- Comply with the policies and guidelines for any specific set of resources to which access has been granted. When other policies are more restrictive than this policy, the more restrictive policy takes precedence.

In contrast, misuses include but are not limited to:

- Using an unauthorized computer account.
- Using the District network to gain unauthorized access to any computer systems or information.

- Knowingly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly running or installing on any computer system or network, 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, and worms.
- Attempting to circumvent data protection schemes or uncover security vulnerabilities.
- Violating terms of applicable licensing agreements.
- Using electronic mail to harass others.
- Masking the identity of an account or machine.
- Posting materials online that violate existing local, state and federal laws or District policies.
- Attempting to maliciously monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software.
- Using District resources for commercial purposes or for personal financial gain.
- Using District resources for creation or distribution of unauthorized promotional materials or other forms of solicitation.
- Accessing restricted portions of the network, an operating system, security software or other administrative applications without appropriate authorization by the system owner or administrator.
- Developing or using programs that may disrupt other computer or network users or that damage software or hardware components of a system.
- Downloading and/or using tools that are normally used to assess security or to attack computer systems or networks (e.g., password "crackers," vulnerability scanners, network sniffers, etc.) unless specifically authorized to do so by the Technology and Computer Services Department.
- Connecting unapproved devices to the network.

Adherence with Federal, State and Local Laws

All existing laws (federal, state and local) and District policies and administrative procedures apply, including not only those laws, policies and procedures that are specific to computers and networks, but also those that may apply generally.

All computer and information technology equipment, including software and data communication links owned by the District, are District property.

Privacy and Personal Rights

Users should be aware that they have no expectation of privacy in the use of the District network and computer resources. The District reserves the right to monitor all use of the District network and computer resources to assure compliance with

these policies. The District will exercise this right for only legitimate District purposes, including but not limited to ensuring compliance with this procedure and the integrity and security of the system.

District employees and others are prohibited from "seeking out, using, or disclosing" personal information contained in electronic records without authorization. All users are required to take necessary precautions to protect the confidentiality of personal information encountered in the performance of their duties or otherwise. If personal information is inadvertently encountered, the individual encountering the information shall not further disclose this information to another individual unless this information reveals a possible violation of laws or regulations, in which case that individual shall report the situation to his or her supervisor.

This procedure does not address the ownership of intellectual property that has been created by employees of the District for use in performing their job responsibilities or intellectual property that has been created by employees using District technology resources. Ownership of intellectual property is governed by law and other District policies, procedures, and contracts.

User Compliance

Misuse of computing, networking, or information technology resources may result in the loss of access to computing resources. Users may be held accountable for their conduct under any applicable District policies, procedures, or collective bargaining agreements, as well as federal, state and local laws. Complaints alleging misuse of District resources will be directed to the appropriate supervisor or administrator.

Title IV Information Security Compliance

- A designated employee or employees to coordinate the District's information security program.

- Identification of reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of an individual's 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 District'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 District 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 individual's information at issue; and

(2) Requiring the District’s service providers by contract to implement and maintain such safeguards.

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

Board Approved	05/04/2010
Board Revised	05/03/2016
Revised	07/21/2020
Board Approved	04/08/2025