AP 3720 Computer and Network Use Procedure – District Employees

Reference:

17 U.S. Code Sections 101 et seq.;
Penal Code Section 502, Cal. Const., Art. 1 Section 1;
Government Code Section 3543.1 (b)
Federal Rules of Civil Procedure, Rules 16, 26, 33, 34, 37, 45

1. Computer and Network Use Procedure

I. Introduction

The District is committed to providing access to computing resources to all current employees. In order to comply with federal and state regulations, laws, and harassment mitigation policies, the District is establishing these procedures for the appropriate use of District Systems.

II. Definitions

A. "District Systems" means all District owned and maintained electronic technology including, but not limited to, computer hardware and software, electronic devices such as tablet computers, smart phones and cell phones, telephone and data networks (including intranet and Internet access), e-mail systems, and electronically stored data. The definition of District Systems

expressly includes access to District data networks, including intranet and Internet access, and District e-mail systems, from devices owned by a User or the District, whether on or off District property.

B. "System Administrator" means staff employed by the District whose responsibilities include system, site, or network administration and staff employed by the District departments whose duties include system, site or network administration. System Administrators perform functions including, but not limited to, installing hardware and software, managing a computer or network, and keeping District Systems operational.

C. "User" means someone who does not have System Administrator responsibilities for District Systems.

D. "User Account" means the combination of a user number, user name, or user ID and a password that allows an individual User access to District Systems.

III. Scope

This policy applies to any employee who uses the District Systems. This policy applies to all use of and access to District Systems from off campus and on campus, as well as access to District Systems from privately owned computers and electronic devices.

IV. Rights and Responsibilities

Use of District Systems is a privilege governed by certain regulations and restrictions as defined by the District as well as all applicable federal, state and local laws.

This administrative procedure will govern use of the District System by District employees as indicated in Board Policy 3720. The User agrees to abide by the regulations set forth in this policy. This means that the User agrees to behave responsibly according to the standards established by the District and this document while using District Systems. Conduct that violates this policy is listed in Section VI. Inappropriate Use.

V. Appropriate Use/Guidelines.

Activities deemed to be appropriate uses of District Systems include the following:

A. Instructional use:

1. Use in classroom instruction.

2. Development of instructional materials.

3. Research connected to academic and instructional concerns and interests.

4. Communication with colleagues, students and professional organizations and institutions if such communications are related to the business of the District.

B. Administrative Use:

1. District administrative and business communications and transactions.

2. Communication with colleagues, students and professional organizations and institutions if such communications are related to the business of the District.

3. Research tied to District concerns and interests.

VI. Inappropriate Use.

District Systems are shared and limited resources. All users have an obligation to use these resources responsibly. Certain activities are prohibited, including but not limited to:

A. Unauthorized use of a User Account.

B. Using District Systems to gain or attempt to gain unauthorized access to any computer systems, or gaining or attempting to gain unauthorized access to District Systems themselves.

C. Connecting unauthorized equipment to the District Systems.

D. Unauthorized attempts to circumvent data protection schemes or uncover security loopholes in within or outside of District Systems. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.

E. Knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks, whether within or outside of District Systems (e.g., deleting programs or changing icon names).

F. Knowingly or carelessly running or installing on any District Systems, or giving to another user or using District Systems to transmit, 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.

G. Deliberately wasting/overloading computing resources on District Systems, such as printing too many copies of a document.

H. Violating terms of applicable software licensing agreements or copyright laws on District Systems.

I. Violating copyright laws and their fair use provisions using District Systems through inappropriate reproduction or dissemination of copyrighted text, images, etc.

J. Using District Resources for commercial activity, such as creating products or services for sale.

K. Using electronic mail via District Systems to harass or threaten others. This includes sending repeated, unwanted e-mail to another user.

L. Initiating or propagating electronic chain letters via District Systems.

M. Inappropriate mass mailing via District Systems. This includes multiple mailings to newsgroups, mailing lists, or individuals, e.g. "spamming," "flooding," or "bombing."

N. Forging the identity of a user or machine in an electronic communication via District Systems.

O. Transmitting or reproducing materials that are slanderous or defamatory in nature or that other-wise violate existing laws or college regulations via District Systems.

P. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software via District Systems without the explicit agreement of the owner.

Q. Transmitting pornographic material via District Systems.

R. Pirating of computer software via District Systems.

VII. Privacy

Users of the District Systems, including the Internet and email, should not expect, nor does the district guarantee, privacy for email or any use of the District Systems. The District reserves the right to access and view any material accessed or stored on District Systems or any material used in conjunction with its District Systems even if that material is stored on a devise that is not owned by the District. Employees are also reminded that electronically generated content produced by District employees may also be subject to the California Public Records Act, and may be subject to public disclosure.

The District does not routinely engage in active key work monitoring or search of emails and contents submitted, however, the District reserves the right to monitor the usage of all District Systems to ensure compliance with this policy, college policy, and federal, state and local laws. User files and information on District Systems may be subject to search by law enforcement agencies under court order if such files contain information which may be used as evidence in a court of law.

District Users are expected to comply with copyright and intellectual property laws.

Users who become aware of any violation of this policy should notify the proper authorities. These authorities include the appropriate administrator, the Office of the Superintendent/President, and/or the local police.

VIII. Enforcement

Violations of this policy will be reported to the appropriate administrator and, if warranted, the appropriate civil authorities. Non-compliance with this policy may also result in cancellation of a User Account and loss of access to District Systems, adverse employment actions, and legal action.

IX. Indemnification/Liability Statement

The District makes absolutely no warranties of any kinds, either express or implied, for the District Systems it provides. The District will not be responsible for any damages suffered by Users, including, but not limited to, any loss of data resulting from delays, non-deliveries, user errors, hardware or software failures, or service interruptions caused by the District's Systems. The District does not service personal computers nor provide technical support for personal devices.

Use of any information obtained via the District's Systems is at the User's own risk.

The District is not responsible for any damage to your personal electronic devices due to any power problem while on campus, or interaction with the District Systems. Further, the District is not responsible for damage or theft of electronic devices under your control.

The User agrees to indemnify and hold harmless the District, the Board of Directors, and District employees from and against any claim, lawsuit, cause of action, damage judgment, loss, expense, or liability resulting from any claim, including reasonable attorneys' fees, arising out of or related to the use of the District Systems. This indemnity shall include, without limitation, those claims based on trademark or service mark infringement, trade name infringement, copyright infringement, defamation, unlawful discrimination or harassment, rights of publicity, and invasion of privacy.