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

I. Computer and Network Use Procedure

I. Introduction
II. Definitions
III. Scope
IV. Rights and Responsibilities
V. Appropriate Use/Guidelines
VI. Inappropriate Use
VII. Privacy

VIII. Personal Use
IX. Confidentiality

X. Electronic Messaging

XI. Social Networking Technologies

XII. Use of District Assets

XII. Enforcement

IX. Indemnification/Liability Statement

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.
   • Development of instructional materials.
   • Research connected to academic and instructional concerns and interests.
   • 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. **Illegal activities.**

B. **Unauthorized use of a User Account.**

C. **Sharing of usernames and/or passwords.**

D. 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.

E. Connecting unauthorized equipment to the District Systems.

F. 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.

G. 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).

H. 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, and other forms of malware including ransomware.

I. Disabling software designed to prevent viruses or malware or disabling screen savers or encryption methods.

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

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

Commented [AP1]: Comment from John E.: I believe that the statement as it stands is too vague. One would need a definition of "too many". Otherwise, anything could be deemed "too many" and the consequences could follow.

How does one define "overloading computing resources"? Watching a video? Downloading an audio file? Printing one sides pages when two sides would conserve resources?
L. 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 otherwise 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. Downloading or transmitting pornographic material via District Systems.

U. Pirating of computer software via District Systems or intended for District use only.

V. Leaving confidential or sensitive materials in plain sight without taking protective measures.

W. Transferring or storing information on untrusted third-party servers.

X. Providing information about, or lists or organizational charts of District employees to external parties.

VII. Privacy

Commented [AP2]: Comment from John E.: Forwarding a link of a speech by Hitler for a History class would qualify as transmitting defamatory material.

Commented [AP3]: Comment from John E.: What defines "in plain sight"? On a computer screen? In a trash can? What defines "confidential"? What defines "sensitive"?

Commented [AP4]: Comment from John E.: Is Google a trusted third party? Yahoo? Microsoft?

Commented [AP5]: Comment from John E.: This is by far the most ridiculous: By this definition, if a book representative sends me a copy of a Psychology book and I reply that I am not a Psychology professor and that it would be better to contact Dr. Oja, I could be reprimanded, which is patently absurd. Moreover, org charts and other plans of this nature are freely available in places on our Internet site. This provides the means to reprimand employees for providing information to someone even though that information might be helpful or freely available. To think that all of our salaries are available through Transparent California but that we could be reprimanded for sharing the name of the president of Taft College is beyond absurd: it is abusive.
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 device 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 keyboard 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. The Superintendent/President is the only one who can request access to an email account. Email accounts may be requested during an investigation or in an instance when the College is served a subpoena for emails. If the investigation is about the Superintendent/President, the Board of Trustees President may request access to the necessary email accounts.

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. **Personal Use**

Computers and computer accounts given to users are provided to assist district employees and volunteers in the performance of their jobs. All computer systems belong to the District and are intended for business and instructional use. Users are expected to exercise good judgment regarding the reasonableness of personal use of District information systems and assets. Personal use should not conflict in any way with business objectives or interests, organizational values, or standards of business conduct. The District reserves the right to limit or prohibit the use of any software not licensed or approved by the District. If unlicensed software is found to reside on a District computer, it must be removed.
The District considers all information transmitted through or stored in its business system, including e-mail, instant messaging (IM) or chat data, and voice mail messages, as District business information. All files and other business information stored on District systems, even if considered “personal” by an employee, are and remain the property of the District. The District may review or use such business information as it deems appropriate.

IX. Confidentiality
Sensitive, personally identifiable, and student information are considered confidential and must remain confidential at all times. This information is accessible only to those District staff who need such access in order to perform their jobs, or to others who have been expressly authorized by the District for specific limited purposes. Unauthorized disclosure of confidential information could cause great harm to the District and may be protected by law.

Confidential must be protected from disclosure to third parties (non-employees) by default. Third parties may be given access to District information only when a demonstrable need-to-know exists. Such disclosure may be authorized by District management or by contract, such as with a temporary worker, consultant, or service provider. A non-disclosure agreement may be required as directed by the relationship and District legal requirements.

Confidential information may be stored in designated locations only and must be securely deleted when it is no longer required. If stored on portable devices such as a flash drive, confidential information requires encryption so that it cannot be read by unauthorized persons. Confidential information that is on paper or other media must also be stored securely.

Specific information about the District’s computer network, information system security, security controls, or potential vulnerabilities may not be distributed to persons who do not have a demonstrable need-to-know, and without prior approval from the District.

All information systems assets provided by the District remain the sole property of the District. Any data or intellectual property created by the user, including
voicemail and electronic messages, remain the property of the District and should not be removed, copied or shared with any person or entity except as part of the user’s normal job responsibilities.

X. Electronic Messaging
The District has an electronic mail (e-mail) network and instant messaging (IM) services. Users are responsible for using these technologies responsibly and within the following guidelines:

A. The District’s e-mail system is not to be used to solicit for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.

B. Sending unsolicited e-mail messages is prohibited, including the sending of junk mail or other advertising material to individuals who did not specifically request such material.

C. Creating or forwarding chain letters or pyramid schemes of any type is prohibited.

D. Users must not create any messages that may be considered offensive or disruptive. Examples of messages deemed to be offensive are any which contain sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone’s age, sexual orientation, religious or political beliefs, national origin or disability.

E. District business communications transmitted by e-mail must use the appropriate District e-mail address (userid@taftcollege.edu) and employ the standard e-mail signature for external communications. Falsifying e-mail headers or routing information so as to obscure the origins of the e-mail or identity of the sender is a violation of this Administrative Regulation.

F. Because e-mail records and computer files may be subject to discovery in litigation, users must avoid making statements in e-mail that would not reflect favorably on the District if disclosed in litigation or otherwise. Delete unnecessary e-mail promptly.

Commented [AP10]: Comment from John E.: As it stands, this implies that research conducted by a professor would belong to the college, which conflicts with every known policy of institutions of higher education. As it stands, if a professor were to write a textbook, the district would own that book and have the ability to collect royalties on that book.

Commented [AP11]: Comment from John E.: Needs definition. Any message I send, such as, “Do you want to have lunch today?” would be unsolicited.

Commented [AP12]: Comment from John E.: This places the onus of defining “offensive” on the potential offended, which provides far too much latitude.

Commented [AP13]: Comment from John E.: I am at a loss for words.
G. Unauthorized access to others’ e-mail accounts is prohibited.

H. Confidential information (sensitive, personally identifiable, or student information) must not be e-mailed over public networks or stored on portable devices such as flash drives without encryption.

I. Caution must be used when opening e-mail attachments or following hypertext links received from unknown senders, which may contain malware or viral code.

XI. Social Networking Technologies

Social networking tools (blogs, online social networks, Facebook, Twitter, etc.) provide an open exchange of information and a means to establish relationships with colleagues and members of the public. These tools represent a communication model where a fine line exists between business and personal statements.

IX.XII. 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.

X.XIII. 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.

Working Copy 11/5/19
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/Trustees, 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.