HARTNELL COMMUNITY COLLEGE DISTRICT

AP 3720 Computer, Electronic Communication, and Network Use

References: 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

In support of the College's mission of teaching, research, and public service, Hartnell provides computing, networking, and information resources to the campus community of students, faculty, and staff.

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 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 laws, regulations, and contractual obligations.

Students, employees may have rights of access to information about themselves contained in computer files, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access user files as required to protect the integrity of computer systems. For example, following organizational guidelines, system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged.

Existing Legal Context

All existing laws (federal and state) and District regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct. Misuse of computing, networking, or information resources may result in the restriction of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable District or campus policies, procedures, or collective bargaining agreements. Complaints alleging misuse of campus computing and network resources will be directed to those responsible for taking appropriate disciplinary action. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment.

Examples of Misuse

Examples of misuse include, but are not limited to, the activities in the following list.

a) Violation of Law. Any use of Hartnell's technology resources which is in violation of federal, state or local law, or which is in aid to or furtherance of the violation of federal, state or local law, is prohibited. This includes, but is not limited to, the violation of copyright and other intellectual property laws.
b) Using a computer account that you are not authorized to use. Obtaining a password for a computer account without the consent of the account owner.
c) Using the Campus Network to gain unauthorized access to any computer systems.
d) Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
e) 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.
f) Attempting to circumvent data protection schemes or uncover security loopholes.
g) Violating terms of applicable software licensing agreements or copyright laws.
h) Deliberately wasting computing resources.
i) Using electronic mail to harass others.
j) Masking the identity of an account or machine.
k) Posting materials on publically accessible information technology resources that violate existing laws or the District's codes of conduct.
l) Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
m) Commercial Activities. Hartnell's technology resources exist for educational purposes and may not be used for any commercial activities for personal financial gain, whether on behalf of individuals or for-profit entities, unless expressly authorized by Hartnell in writing.
n) Obscene Material. Accessing, uploading, downloading, transmitting, producing, storing or viewing of any obscene material is prohibited. Obscene material includes "harmful matter" as defined by California Penal Code section 313, meaning "matter, taken as a whole, which to the average person, applying contemporary statewide standards, appeals to the prurient interest, and is matter which, taken as a whole, depicts or describes in a patently offensive way sexual conduct and which, taken as a whole, lacks serious literary, artistic, political, or scientific value for minors."
o) Food or Drink Prohibited. Users of Hartnell's technology resources generally accessible to the public, such as computer labs, may not possess or consume any food or drink, including water, while using such resources or within the immediate vicinity of the technology equipment.
p) Defamatory/Harassing/Threatening Material. Creation or transmission of material which is defamatory, harassing or threatening toward another person is

prohibited. Using Hartnell's technology resources to violate the legal privacy rights of any individual is also prohibited.

Activities will not be considered misuse when authorized by appropriate District officials for security or performance testing.

Additional Use Policies

The Computer Use Policy applies to use of all Hartnell Campus computing resources. Additional computer and network use policies and terms and conditions may be in place for specific electronic services offered by the campus. The Computer Use Policy applies to the use of Hartnell computers and networks for electronic communications. Users must familiarize yourselves with any of these when you agree to use these services.

Authorized Use by Minors

Hartnell students under the age of eighteen, by accepting the benefits of authorized use of the District's technology resources, acknowledge that material inappropriate for minors is accessible on the Internet; that various wrongdoing, such as identity theft, invasion of privacy and fraud, may occur on the Internet, and that their use of the Internet may therefore expose them to a variety of risks of harm to person or property. By using Hartnell's technology resources, minors and their parents accept responsibility for any and all risks thereof and acknowledge that Hartnell shall not be responsible for any harm or damage resulting from such use.

Web Pages

Hartnell College has established and presently maintains a web site which includes information regarding Hartnell's mission and purpose, courses, faculty and staff, students, and such other information and resources as the Hartnell administration determines is appropriate for inclusion (this includes a public listing of employee directory/contact information). The use of Hartnell technology resources for the creation of individual web pages, whether for official or personal purposes, shall be subject to the following requirements:

a) Establishing Official Web Pages. The Hartnell administration may authorize a process for the creation and maintenance of official web pages by Hartnell faculty, staff, departments of the College, or student organizations. Official web pages must be approved by the designated Hartnell administrator and the content must be consistent with the general style and content of the Official Hartnell web site. The addition or modification of material to official web pages must also be approved by the designated Hartnell administrator prior to the posting of such content. Material appropriate for placement on official web pages includes administrative and academic information for specific departments or student organizations, faculty, staff or class information, or relevant reference information. Official pages must be served from officially

designated server platforms that the IT personnel has authorization and access to for maintenance or content management.

b) Establishing Personal Web Pages. The Hartnell administration may authorize the creation and maintenance of personal web pages by students, faculty or staff. Personal web pages must be for educational purposes, including research, discussion, academic development, public service and other educational uses consistent with the mission of Hartnell, and must otherwise comply with the requirements of this technology use policy. The creation of personal web pages must be authorized by the appropriate administrator and proposed content may be reviewed for compliance with this policy. In addition to the requirement that the content of personal web pages comply with this policy, any sites to which the personal web page links must be consistent with this policy.

c) Personal Web Page Disclaimer. Personal web pages must include the following notice: "This is a personal web page. Any opinions expressed on this page are not those of Hartnell College, nor does Hartnell guarantee the accuracy or appropriateness of any information contained on this page, nor any information linked to by this page."

Email Correspondence

Email correspondence between employees of the Hartnell CCD, between employees and students, and between employees and external entities (e.g., vendors, community members) directly related to performing job duties and conducting the business of the District must take place using the official @hartnell.edu email address. Communications between enrolled students and employees must utilize the @student.hartnell.edu email address. Hartnell College students should be directed to check @student.hartnell.edu email often for communication from the college and its employees. There are exceptions to this procedure such as when employees are contacted by past students who no longer use or prospective students who have not yet received their @student.hartnell.edu email address. There can also be occasional situations when communicating with the official Hartnell email address is not possible due to computer network outages or other circumstances.

Internet and E-mail access is a privilege, not a right, and activities that may be acceptable on your private account at home may not be acceptable when using your District-authorized service.

As a public institution, the Hartnell CCD is subject to the California Public Records Act (Government Code § 6250 et seq.). The PRA requires that all communications related to public business "regardless of physical form or characteristics, including any writing, picture, sound, or symbol, whether paper, magnetic or other media" be made available to the public. This means that any member of the public can request copies of email communications that have been produced by any employee or student of the District. There are exemptions for disclosure of public records and they generally include personnel records, investigative records, drafts, and material made confidential by other

state or federal statutes. Setting aside these few exemptions, the vast majority of email communications are available through a PRA request. Therefore, email communications among and between employees and/or students are not confidential or private. Placing a "confidential statement" at the end of an email does not control whether a communication is exempt from the PRA. Email communications related to HCCD business can be distributed and/or forwarded without permission of the sender.

When system problems occur, such as hardware or software failure or attacks by malicious users, the IT staff, who maintain the e-mail servers, are authorized to look at any information and any files on District computers that are necessary to solve the problems and to protect the systems and the information they contain. It is part of the system administrator's job to do this and to treat any information on the systems as confidential.

In addition to the authorized actions of the District's system administrator, e-mail can end up in the hands of computing staff if it was inaccurately addressed and if it could not be delivered.

Personal Use of Computer and Network Resources
Brief and occasional personal use of District computer and network resources is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the District or otherwise violates District policy or procedure.

Appropriate Use
Hartnell extends to students, faculty, and staff the privilege to use its computers and network. When you are provided access to our campus network, you are enabled to send and receive electronic mail messages around the world, share in the exchange of ideas through electronic news groups, and use Web browsers and other Internet tools to search and find needed information.

The Internet is a very large set of connected computers, whose users make up a worldwide community. In addition to formal policies, regulations, and laws that govern your use of computers and networks, the Internet user community observes informal standards of conduct. These standards are based on common understandings of appropriate, considerate behavior that evolved in the early days of the Internet, when the internet was used mainly by an academic and highly technical community. The Internet now has a much wider variety of users, but the early codes of conduct persist, crossing boundaries of geography and government, in order to make using the Internet a positive, productive, experience. You are expected to comply with these informal standards and be a "good citizen" of the Internet.

Enforcement
Penalties may be imposed under one or more of the following: California Education Code regulations, Hartnell regulations, California law, or the laws of the United States. Minor infractions of this policy or those that appear accidental in nature are typically handled informally by electronic mail or in-person discussions. More serious infractions are handled via formal procedures. In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation. Infractions by students may result in the temporary or permanent restriction of access privileges, notification of a student's academic advisor and/or referral of the situation to the Office of Student Affairs. Those by a faculty or staff member may result in referral to the department head or administrative officer. Offenses that are in violation of local, state, or federal laws may result in the restriction of computing privileges, and will be reported to the appropriate District and law enforcement authorities.

Reporting Misuse
A user who asserts that the District or District personnel have violated this policy shall file a complaint with his or her immediate supervisor with a copy to Human Resources and a copy to the employee's bargaining unit in the event the alleged violator is an employee or Student Affairs in the event the violator is a student. The administration will contact the alleged violator to discuss the complaint. The supervisor/administrator of the complainant shall initiate an investigation if necessary and determine an appropriate remedy/resolution in consultation with the appropriate Vice President. In cases where the supervisor/administrator is part of the complaint, the complaint shall be filed with the next level of supervision for investigation and resolution and/or remedy. The complainant shall be informed in writing 1) of the initiation of the investigation, and 2) of its outcome as appropriate, with copies to the appropriate Vice President and the employee's case the correct bargaining unit. Complainants dissatisfied with the resolution/remedy have full recourse to relevant contractual protections and/or legal action

Dissemination and User Acknowledgment
All users shall be provided copies of these procedures and be directed to familiarize themselves with them.

Students shall acknowledge acceptance of BP/AP 3720 electronically when accessing District computer and network resources. Employees shall acknowledge acceptance of BP/AP 3720 during the employment process.

Disclosure
No Expectation of Privacy
The District reserves the right to monitor all use of the District network systems and computers to assure compliance with these policies. Users should be aware that they have no expectation of privacy in the use of the District network and computer

resources. 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.

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

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.

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 and computer must be disclosed if requested by a member of the public.

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

See Board Policy 3720

Approved by the Superintendent/President: April 2, 2014

Computer and Network Use Agreement

I have received and read a copy of the Hartnell Community College District Administrative Procedure 3720, Computer and Network Use, adopted by the Board of Trustees, and recognize and understand the guidelines.

I agree to abide by the standards set in the procedure for the duration of my employment and/or enrollment.

I am aware that violations of this Computer and Network Use Procedure may subject me to disciplinary action including, but not limited to, revocation of my network account up to and including prosecution for violation of State and/or Federal law.

_____

Signature Date

_____

Name (Printed)