ROBERT J. BEZEMEK
PATRICIA LIM
DAVID CONWAY

LAW OFFICES OF
ROBERT J. BEZEMEK
A PROFESSIONAL CORPORATION
THE LATHAM SQUARE BUILDING
1611 TELEGRAPH AVENUE, SUITE 936
OAKLAND, CALIFORNIA 94612-2140
Telephone: (510) 763-5690 ● Facsimile: (510) 763-4255

Proposed Computer Use Agreement/Policy

March 2012

1. GUIDING PRINCIPLES

The Peralta Community College District (PCCD) recognizes that principles of academic freedom and shared governance, freedom of speech, employee rights to engage in union and concerted activities under the EERA, Constitutional rights of privacy under the California Constitution, and privacy of information, hold important implications for electronic mail and computer services.

a. The PCCD affords electronic mail and Computer services privacy protections comparable to that which the law traditionally affords paper, sealed mail and telephone communications, and personal storage such as briefcases either owned by, or under the control of, individuals.

b. The PCCD encourages the use of electronic services by its employees for purposes of efficiency, convenience and exercise of rights, and respects the privacy of its users.

c. The PCCD does not routinely inspect, monitor, or disclose electronic mail without the holder's consent.

d. Faculty have a reasonable expectation of privacy in computer usage, including emails, sent or received from privately owned computers, and in private communications from district-provided computers for which such communications are expected.

2. PURPOSE

The purpose of these guidelines is to assure that:

a. The rights of users of computers or other electronic resources are protected, including faculty users' constitutional rights of, and rights to engage in freedom of speech, union activities , or concerted activities.

b. The PCCD community is informed about the applicability of these guidelines to electronic mail and computer services;

c. Electronic mail and computer services are used in compliance with these guidelines;

d. Users of electronic mail and computer services are informed about how privacy and security apply to their electronic mail;

e. Disruptions to PCCD electronic mail and computer and other services and activities are minimized.

3. CAUTIONS

Users should be aware of the following:

a. Notwithstanding the protection afforded privacy and other rights in this policy, electronic communications are generally less private than users may anticipate due to worms, viruses, security matters and related issues.

b. The PCCD cannot and does not wish to be the arbiter of contents of electronic mail and computer services. Neither can the PCCD, in general, protect users from receiving electronic mail they may find offensive. Users are advised that they may encounter material which may be considered offensive or objectionable in nature or content. Users are further advised that PCCD does not assume responsibility for the contents of any private or public outside networks.

c. There is no guarantee that electronic mail received was in fact sent by the purported sender, unless authenticated systems are in use. As with print documents, in case of doubt receivers of electronic mail should check with the purported sender to validate authorship or authenticity.

d. PCCD is not responsible for backing-up files from an individual's computer system. Users who wish to have backup storage for data on their machines must provide their own backup measures.

4. SCOPE

These guidelines apply to:

a. All electronic mail and computer services provided or owned by the PCCD;

b. All users, holders, and uses of the PCCD electronic mail and computer services;

c. All PCCD electronic mail records in the possession of PCCD, its employees or other users of electronic mail and computer services provided by the PCCD.

d. A "user" is a member of the faculty or other individual or entity authorized or permitted to use PCCD computer resources.

5. GENERAL PROVISIONS

As noted in the Introduction, the PCCD recognizes that principles of academic freedom, freedom of speech, rights to engage in union and concerted activities, and right of privacy, and privacy of information hold important implications for electronic mail and computer services.

a. These guidelines do not waive any user rights protected by state or federal law, including rights of privacy.

b. The District shall not inspect or monitor computers and computer-related matter, including but not limited to equipment, software, websites, access to websites, hardware, or related matter, which is not owned by the District.

c. A designee of PCCD must approve all access to PCCD's computer resources, including the issuing of passwords.

d. The authorized user is responsible for the proper use of the system, including maintaining the security of password protection.

e. Users may not transfer or confer these privileges to non-users, absent permission or authority to do so.

f. Any attempt to increase the level of access to which s(he) is authorized, or any attempt to deprive other authorized users of resources or access to any PCCD computer system shall be regarded by the PCCD as a violation of these guidelines.

g. Any user who finds a possible security lapse on any computer system is obligated to report it to their immediate supervisor. Once reported the PCCD is responsible for securing the system until a system administrator or designee has investigated the problem.

h. Users should be aware that during the performance of their duties network

and computer operations personnel and system administrators need from time to time to observe certain transactional addressing information to ensure proper functioning of PCCD electronic mail and computer services, and on these and other occasions may inadvertently see the contents of e-mail messages. Except as provided elsewhere in this guidelines they are not permitted to see or read the contents intentionally; to read transactional information where not germane to the foregoing purpose; or disclose or otherwise use what they have seen. Information protected by the right of privacy or other rights, which is inadvertently accessed, shall be kept confidential and shall not be used to adversely affect faculty members.

i. Computer software protected by copyright is not to be copied from, into, or by using PCCD Computer facilities, except as permitted by law or by the contract with the owner or licensee of the copyright. This means that such computer and microcomputer software may only be copied in order to make backup copies, if permitted by the copyright owner. In addition, the number of software copies cannot exceed the total number that have been purchased or licensed.

j. Personal Use: PCCD electronic mail and computer services may be used for personal purposes provided that, in addition to the foregoing constraints and conditions, such use does not directly interfere with the PCCD operation of computer facilities or electronic mail services, and shall generally occur during non-work time.

Use includes use of district computers for private communications, or communications protected by law, including laws protecting union and concerted activities or freedom of speech.

Other authorized communications include communications from a private computer sent over the district server or network, or communications from a district owned or controlled computer, which are private communications or activities of the faculty member.

Incidental use during working time is permitted when there is no reasonable alternative - e.g. family emergency, unavoidable need for personal affairs - i.e. essential financial transactions, medical needs.

k. These guidelines do not address the ownership of intellectual property stored on or transmitted through PCCD electronic communication resources.

6. PROVISIONS FOR INSPECTING AND MONITORING COMPUTERS

a. The PCCD may inspect, monitor, and disclose electronic records only when each of these conditions are met:(i) such action is required and consistent with law, including court decisions concerning monitoring of telephonic communication; and, (ii)

there is a substantiated reason to believe that violations of law, or these guidelines, have taken place;(iii) the District has reasonable evidence to believe that the individual has violated the law or these guidelines (individualized suspicion shall be required); and, (iv) the inspection, monitoring or disclosure does not violate the privacy rights of faculty as provided herein; and (v) PCCD has obtained a search warrant.

b. Where a district computer or related equipment is provided to the faculty member in regard to his/her employment, said individual shall be permitted to use the computer/equipment for reasonable personal use. The District shall not inspect any personal material saved, stored, retained or distributed by said computer or equipment without a search warrant, and employees have an expectation of privacy in their personal material.

c. In any instance in which a violation of criminal law is or should reasonably be suspected, the District shall be required to obtain a search warrant in accordance with judicial safeguards, to conduct inspection of a computer or computer records.

d. Notwithstanding the foregoing provisions, the PCCD is not authorized to, and shall not inspect or monitor computers or computer-related hardware, software, programs, equipment or devices, which are not owned by the PCCD.

e. Only the PCCD Chancellor, or designated Vice-Chancellor, may authorize inspection or monitoring after making a prior written finding citing substantial reason to warrant it and individualized suspicion, or when required by a subpoena. Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

(1) The PCCD shall seek the consent of the user before seeking to, or allowing, inspection, monitoring or disclosure of electronic records.

(2) If a need arises to divert, inspect or monitor or disclose computer records or email messages from or to a faculty member, both the sender and recipient should be notified in ample time for them to object to disclosure, or to pursue protective measures such as judicial relief, except for the rare case where such delay would create an imminent threat or risk to human safety or college property. [Source: AAUP draft policy]

(3) The PCCD shall only seek or permit the inspection, monitoring, or disclosure of electronic records without the consent of the holder of such records (i) when required and consistent with the law; (ii) when there is a substantiated reason to believe that violations of law or the PCCD guidelines have taken place. Where non-consensual inspection, monitoring, and disclosure of electronic records held by faculty is

involved, the advice of the Generic Faculty Association (UFA)shall be sought in writing in advance. All such advice shall be sought in a timely manner.

(4) The responsible authority or designee shall, at the earliest possible opportunity that is lawful and consistent with these guidelines, notify the affected individual of the action(s) taken and the reason(s) for the actions taken. The UFA shall be copied on this notice when it is to a faculty person.

(f) The PCCD inspection and/or monitoring is limited to those computer systems for which the PCCD has a substantiated reason to believe they were used in violation of law and/or these guidelines. Inspection, monitoring, and disclosure will be limited to investigation of the substantiated reason(s).

(g) Monitoring shall be limited to the least amount of time necessary to resolve the situation and shall not exceed a two-week period unless there is substantiated reason or a legal requirement to continue.

(h) The contents of any messages or material inspected or accessed may not be used or disseminated more widely than the basis for such use or dissemination may warrant. However, in every instance, the individual whose messages or material has been inspected or accessed shall be immediately notified of the precise material inspected, accessed, copies or retained. The exclusive bargaining agent of said individual shall be concurrently informed.

(i) The District shall not suspend, or terminate a faculty members access to district computer resources, or in any way punish a faculty member in regard to his/her use of computer resources, without a hearing before a reasonably objective district official, in which the District shall bear the burden of proof. The employee shall be provided with notice of all charges upon which the action is based, and shall be entitled to legal representation. The hearing shall be held within a reasonable time after the issuance of any order to suspend, terminate or punish. Any decision to suspend or terminate shall be subject to the grievance procedure.

Faculty Owned Computers and Non-District Computers

e. The PCCD may only inspect, monitor, or obtain electronic communications, stored on a computer owned by the faculty member, or not owned by the District, by obtaining a search warrant in accordance with the requirements of State law.

f. The PCCD shall not access, without a search warrant, communications of faculty, including stored communications, sent from a private computer through the PCCD computer network, to a non-District computer; or information stored on a non-District server (i.e. googlemail, aol mail, etc.).

District Owned Computers Within the Control of Faculty

g. The following rules shall apply to computers owned by the District, but under the control of a faculty member, if the District desires to review material stored on the computer:

i. Any portions of a District-owned computer which are identified or designated as "private" by the faculty member, shall be treated as though the faculty member owns the computer. (See above)

ii. As to information not saved within private folders or directories of a District-owned computer, the District may access the information provided

a) there is a strong probability of wrongdoing by the employee.
b) the access must be limited in scope and duration, and for the specific purpose of obtaining the contents of electronic data likely to be directly relevant to the alleged wrongdoing.
c) a relatively neutral and detached authority within the District determines that the access is essential and that probable cause of wrongdoing exists.
d) any information obtained which is not directly relevant to the matter under review or investigation shall be promptly returned to the employee, and no copies shall be retained.
e) the employee shall be notified of what has been retained
f) before the computer is inspected, the employee shall be notified so that s/he has sufficient time to seek judicial intervention to prevent access.

7. EXAMPLES OF MISUSE OF ELECTRONIC MAIL AND COMPUTER SERVICES

Examples of misuse include the activities in the following list, and those added by mutual agreement of the PCCD and the PFT:

a. Using a computer account without authorization.

b. 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. Masking the identity of an account or machine. However, anonymous internet speech is protected by law.

i. Posting materials that violate existing laws on electronic bulletin boards.

j. 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.

Z:\Documents\2300-Peralta\2367-computer use policy negos\2367-2012-REVISED MODEL COMPUTER USE POLICY - RJB V 1 03-22-12.wpd