ADMINISTRATIVE PROCEDURES No. 311.1

MENDOCINO - LAKE COMMUNITY COLLEGE DISTRICT

COMPUTER USE PROCEDURES FOR STAFF AND STUDENTS

1. Computing Resources and Users

   The District provides computers, networks, and computerized records ("computing resources") to students and employees ("users") for the purposes of facilitating education and services.

2. Privacy

   Due to the nature of the technology and the public character of the District's business, there is no guarantee that a user's files, account, and email are private. Documents created and/or stored on District computers and networks may be considered public records, subject to disclosure under the Public Records Act, other laws, or as a result of litigation. While the District does not routinely monitor computer files, electronic mail, or internet use, the District reserves the right to examine material stored on, or transmitted through its computing resources as it deems necessary.

3. Warning About Offensive Material

   Users are warned that when utilizing the Internet, they may encounter material that could be considered offensive or objectionable in nature or content which is beyond the control of the District.

4. User Identifications and Passwords

   A unique user identification and password will be issued to each user for the purpose of accessing computing resources. The security of passwords is essential to the privacy of students and employees. The Director of Computing Services, or designee, shall be responsible for modifying passwords periodically as needed and for canceling access to computer resources as employees' service to the District is terminated and students conclude their need to use computing resources. When user identifications and passwords are issued, users will be provided with a copy of the computer use policy and administrative regulation. **BY ACCEPTING A USER IDENTIFICATION AND PASSWORD, USERS AGREE TO READ AND COMPLY WITH THE POLICY AND REGULATION.**

5. Users shall:

   a. Operate computer resources in compliance with related federal and state law and District policies, rules, and regulations.

   b. Maintain an environment conducive to learning and working by exhibiting the highest standards of professional and personal courtesy while respecting the rights and privacy of others.

      1. <u>Electronic Civility</u>: While the District encourages the free exchange and debate of ideas, it is expected that this exchange will reflect the high ethical standards of the academic community. Users should keep in mind that email is permanent and public. Once a message is sent, it may be saved, printed, or forwarded without the knowledge or consent of the author. Electronic messages should be brief, clear, and professional. The user should take the time to consider the impact of the messages sent. Electronic mail does not convey "body language", facial expressions, or tone so attempts at humor, irony, or sarcasm may be easily misinterpreted.

c. Maintain a secure environment by not sharing passwords or writing them down where other people might have access to them; not leaving computing resources unattended; and immediately reporting to the Director of Computing Services when a password is used by someone other than the user.

d. Back up data and programs to protect files.

e. Make economical and wise use of shared computer resources.

f. Participate in any required training prior to using computing resources.

g. Limit use of computing resources to college related activities and to promote community outreach and volunteerism for non-profit organizations.

6. Policy and Administrative Regulation violations applicable to all users:

a. Utilizing computer resources for non-college related activities except as stated in item 5 g above.

Transferring or extending use of computer resources to people or groups outside the District without the explicit written approval of the Director of Computing Services. Such approval shall be limited to those requests which provide a measurable and necessary benefit to the District.

c. Sending harassing, intimidating, discriminatory, and/or threatening messages through electronic mail or other means.

d. Downloading, storing, or displaying illegal, obscene, or pornographic material, gratuitous violence; material relating to possession and sale of illegal drugs; material on manufacturing of explosive devices; or other material antithetical to the goals and purposes of the District.

e. Using computing facilities in a manner that violates copyrights, patent protections, or license agreements, including using pirated or unlicensed software.

f. Knowingly performing an act which will interfere with the normal operation of computing resources, cause damage, or place excessive load on the system.

g. Connecting any device to the secured network without written approval from Computing Services. The secured network is defined as any “wired” connection.

h. Attempting to circumvent data protection schemes, uncover security loopholes, or gain unauthorized access to any information or files.

i. Intentionally entering, recording, or causing to be recorded any false, inaccurate, or misleading information into the systems.

j. Sending mass advertisements or solicitations, or political mass mailings as defined by the Fair Political Practices Commission.

k. Using computing resources for commercial or personal financial gain.

l. Taking computer hardware or software off campus for any purpose without prior written approval.

m. Personally benefiting, or allowing others to benefit, from any inappropriate access to confidential information.

n. Divulging the contents of any report or record to any person except in the scope and execution of assigned duties and responsibilities.

o. Knowingly including or causing to be included in any record or report a false, inaccurate, or misleading entry; and/or knowingly expunging or causing to be expunged a data entry from any record or report, except in the execution of assigned duties. (While employee users are responsible for entering data into the system correctly, employee users are not responsible for the accuracy of the data assigned to them to be entered.)

p. Removing an official record or report, or copy thereof, from the office where it is maintained except in the performance of assigned duties.

q. Providing printouts of employee, student, and all other college records not in accordance with federal, state, and district privacy rules and regulations and the Public Records Act.

r. Operating computing resources in locations where the display can easily been seen by unauthorized persons.

s. Using computing resources in a manner that violates related state and federal law or District policies, rules, and regulations.

t. Other violations which may be deemed inappropriate by the Superintendent/President.

7. Consequences of Policy and Administrative Regulation Violations

The Director of Computing Services or designee will inform the appropriate supervisor or in the case of students, the Dean of Students of computer use violations. Violations of this regulation will be enforced pursuant to applicable District policies, procedures, and/or collective bargaining agreements.

Misuse may result in the loss of computing privileges; financial restitution to the District for funds expended; and/or disciplinary, civil, or criminal action. Disciplinary action may include the full range of sanctions, up to and including, but not limited to, employee dismissal, student expulsion, and/or legal action. Misuse can also be prosecuted as a criminal offense under applicable statutes, such as Penal Code Section 502 which identifies certain crimes associated with the use of computer systems.

Adopted: May 1, 2002
Revised: May 1, 2007