LOS ANGELES COMMUNITY COLLEGES
OFFICE OF THE CHANCELLOR
ADMINISTRATIVE REGULATIONS   **INDEX NUMBER B-27**

REFERENCE: B-28	TOPIC: Use of District and College Computing Facilities
ISSUE DATE: March 19, 1986	INITIATED BY: Educational Services
CHANGES: All sections; Regulation transferred to Business Services (formerly E-76); Sections I.(E)and III (A);	DATE OF CHANGES: April 1997; August 1, 2005

I. **Policy**

A.   The Los Angeles Community College District provides computers, networks and computerized records ("computing facilities"), for use by students, faculty, staff and administrators. These resources are intended to facilitate education, research, academic development and service to the public. Each individual user of these facilities ("user") is expected to exercise responsibility, use computing resources ethically and respect the rights and privacy of others.

B.   All employees and students using computing facilities are expected to operate within the bounds of federal and state law and of District policies and standards. All existing District rules, regulations and policies apply to the use of computing facilities, including those that apply generally to personal conduct.

C.   The College President or Division Vice Chancellor shall designate an administrator to be responsible for the implementation of this policy.

D.   Each college is responsible for communicating the provisions of this policy to its campus users of computing facilities. Each college may establish guidelines regarding who may use campus computing facilities, consistent with the provisions of this policy.

E.   This policy is intended to supplement Administrative Regulation B-28, the District's Network Security Policy, as appropriate.

II. **Communications and Privacy**

A.   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/or electronic mail 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 or other laws or as a result of litigation. While the District does not routinely monitor computer files, e-mail or Internet use, the District reserves the right to examine material stored on or transmitted through its computing facilities as it deems necessary.

B.   Users are warned that they may encounter material which may be considered offensive or objectionable in nature or content. If a user alleges that a District rule or policy has been violated, he or she may initiate action through the applicable grievance or complaint procedure.

III. **User Responsibilities**

A.   Individual users assume full responsibility and accountability for using computing facilities in accordance with District rules and policies, which includes but is not limited to, compliance with the Policy Violations listed at section IV of this policy. Users must respect the rights of others, respect the integrity of the computing facilities and observe all laws, regulations and contractual obligations.

B.   As a condition of access to computing facilities, every computer user must observe the following guidelines:

1.   Maintain an environment conducive to learning and to working by using computing facilities according to the highest standards of professional and personal courtesy;
2.   Maintain a secure environment for the systems by immediately reporting any security loopholes or unauthorized use of the facilities;
3.   Assume responsibility for the protection of files by backing up data and programs; and
4.   Make economical and wise use of shared computer resources.

C.   Passwords provide employees and students access to computing facilities. The security of passwords is essential to the privacy of students and employees in accordance with State and Federal laws. In order to maintain a secure environment, the following rules should be observed:

1.   A unique user identification and password shall be issued to each individual who is provided with access to computing facilities.

2.   Users should not write their password in any location where another person can find it.

3. Passwords shall be modified periodically as required by the system administrator.

4. In the event a user's identification and password are used for unauthorized purposes by someone other than the user, the user should immediately report the activity to the administrator in charge of implementing this policy.

5. Employees and students shall participate in appropriate orientation and training prior to using computing facilities, when deemed necessary by the College President, Vice Chancellor or the administrator in charge of implementing this policy.

6. Each individual user is completely responsible for all activity on computing facilities performed under his/her identification and password. This is especially critical for those who have access to any of the update systems. Accordingly, computing facilities should not be left unattended.

D. Employees, which includes student workers, may be provided access to computing facilities as part of their assigned duties. Employee users must limit their use of computing facilities to activity within the scope of their employment and necessary to conduct District business.

1. Employee users are prohibited from using computing facilities for inappropriate purposes, which includes, but is not limited to, the following:

a. Employee users are prohibited from personally benefiting or allowing others to benefit from any inappropriate access to confidential information.

b. Employee users are prohibited from divulging the contents of any report or record to any person except in the execution of assigned duties and responsibilities.

c. Employee users may not knowingly include or cause to be included in any record or report a false, inaccurate or misleading entry. Employee users may not expunge or cause to be expunged a data entry from any record or report, except in the execution of assigned duties. Correctly, employee users are not responsible for the accuracy of the data assigned to them to be entered.

d. No official record or report, or copy thereof, may be removed from the office where it is maintained except in the performance of assigned duties.

2. Computing facilities shall not be located in such locations that the display can be seen by unauthorized persons. These locations shall be reviewed periodically by the appropriate administrator.

3. Employee users should not give their personal password to any other person.

4. Employees who do not have a password but have a need for limited and specific use of computing facilities must be under direct supervision of a user who has a password.

5. Printouts of student records shall be provided in accordance with Federal, State and District privacy rules and regulations.

   a. No printout shall be given to a student who does not have proper identification.

   b. "Unofficial" shall be stamped on all computer screen printouts, including study list and permanent record printouts, issued by offices other than Admissions and Records.

6. Printouts of employee records may only be made by users who have been authorized to use the screens in question, and in accordance with Federal, State and District privacy rules and regulations.

7. In order to maintain the privacy of employees and students, the following rules apply with respect to the release of and/or access to student and/or employee records:

   a. The release of and/or access to confidential information shall be made in accordance with Federal, State and District privacy rules and regulations.

   b. Any release of and/or access to computerized records to third parties, in response to an employee's or student's written consent; a lawfully issued subpoena; or a court order, shall be made only by the office directly responsible for such records, under authority of the administrator-in-charge of that office.

8. Upon termination or transfer of an employee, the College President, Division Vice Chancellor or the

administrator assigned to implement this policy shall ensure that access to computing facilities by the employee is terminated or modified, as appropriate.

E.   Students may be provided an account for computer access from the college's designated system administrator and their use shall be limited to college-related activities only.

IV.   **Policy Violations**

Conduct which is considered to violate District policy with respect to computing facilities includes, but is not limited to, the following:

1.   Sending harassing, intimidating and/or threatening messages through electronic mail or other means;
2.   Downloading, storing or displaying obscene or pornographic material;
3.   Using computing facilities in a manner that violates copyrights, patent protections or license agreements, including using pirated or unlicensed software;
4.   Knowingly performing an act which will interfere with the normal operation of computing facilities, cause damage or place excessive load on the system;
5.   Attempting to circumvent data protection schemes, uncover security loopholes or gain unauthorized access to any information or files;
6.   Intentionally entering, recording or causing to be recorded any false, inaccurate or misleading information into the systems;
7.   Sending mass advertisements or solicitations; or political mass mailings as defined by the Fair Political Practices Commission;
8.   Using computing facilities for commercial or personal financial gain;
9.   Taking computer hardware or software from District or college facilities for any purpose without prior written approval; and
10. Using computing facilities in a manner that violates existing state and federal laws or District rules and regulations.

V.   **Consequences of Misuse**

A.   Misuse of computing facilities may result in the loss of computing privileges. Additionally, misuse may require financial restitution to the District for funds expended and could result in disciplinary, civil or criminal action.

B.   Users may be held accountable for their conduct under any applicable District policy, procedure or collective

bargaining agreement. Violations of these policies will be enforced in the same manner as other District policies. Disciplinary review includes 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.

VI. **Guidelines for Electronic Civility**

A. 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. When sending or responding to a sensitive or controversial topic, the user should keep in mind that e-mail is permanent and public. Once a message is sent, it may be saved, printed or forwarded without the knowledge or consent of the author. The user should take the time to consider the impact of all e-mail messages which he or she sends.

B. Electronic mail does not convey "body language," facial expressions or tone so attempts at humor, irony or sarcasm may be easily misinterpreted. Therefore, careful writing is advised. Electronic messages should be brief, clear and professional.

VII. **Applicable Laws and Regulations**

A. The following list identifies some, but not all, of the additional District rules and regulations that apply to the use of computing facilities:

1. Board Rule 9803.26 – Theft or Abuse of Computer Resources
2. Board Rules 1202, 1203 – Nondiscrimination Policy and Complaint Procedures
3. Board Rules, Chapter XV – Sexual Harassment Policy
4. Board Rules, Chapter IX – Article VIII – Conduct on Campus
5. Board Rules, Chapter IX, Article XI – Student Discipline
6. Administrative Regulation E-55 – Student Grievance Procedure

B. This policy supersedes and replaces Chancellor's Directive No. 67, *Guidelines on Use of the LACCD Computer Network*.