

Los Angeles City College Administrative Services "How To" Book	Information Technology Department	IV G-4
How Do I Know Conducts that Violate the College computer Usage and are Prohibited by the College?		

A. How Do I know

The Conducts that violate computer or network usage and are prohibited by the College.

The below listed conducts violate the College computer or network usage policies.

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.
11. 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.
12. The 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.
 13. Employee users should not give their personal password to any other person.

N.B Please note that the below guidelines must be in compliance to avoid any violations.

14. 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.
15. 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.
16. 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.
17. 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.

18. 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.
19. 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. **Reference Administrative Regulations B-27.**
http://www.laccd.edu/admin_regs/