

STUDENT COMPUTER TECHNOLOGY ACCESS AGREEMENT	6515
---	-------------

This is to communicate what other users, instructors, and the District expects of students when using College computer technology and facilities. Failure to conform to these stipulations can result in disciplinary action. Violations of regulations in the use of computer technology will be addressed in accordance with the College Academic Honesty and Student Code of Conduct Policies, available for reference in the College catalog or by requesting copies from Student Services. (The Academic Honesty Policy is also in the class schedule.)

Computer technology and facilities are provided for the purpose of completing academic requirements. Students may use the technology and facilities to:

1. Complete course assignments;
2. Conduct academic research;
3. Communicate with faculty and students.

B. User Responsibilities

User responsibilities include, but are not limited to:

1. Using only their own designated ID, passwords/PIN, and accounts, and keeping IDs, passwords/PIN, and account information confidential. It is recommended that users change their passwords/PIN periodically;
2. Using software and electronic materials, including shareware, in accordance with copyright, trademark, and licensing agreements and restrictions;
3. Accurately identifying and representing themselves in electronic messages, files, and transactions;
4. Saving all work on a floppy disk, zip disk or other removable storage media and not on the hard drive unless instructed to do so by your instructor;
5. Allowing lab technicians to scan disks before they are inserted into the disk drive as a precaution to insure the safety of the computers;
6. Asking appropriate Cuesta College personnel for assistance if unfamiliar with the operating system.

C. Prohibitions

Prohibitions include, but are not limited to:

1. Damaging equipment, data, software, software protection, encryption or restriction on applications and files; including, introducing invasive or destructive programs (such as viruses, worms, and Trojan horses);

2. Disrupting or unauthorized use of accounts, access codes, passwords, or identification numbers;
3. Impeding or disrupting the use of computer technology and communications resources by game playing, sending an excessive or unreasonable number of messages, sending messages of unreasonable size (with large attachments); making or printing excessive copies of documents, files, data, or programs;
4. Violating copyrights, trademarks, and/or license agreements;
5. Accessing, using or copying another user's account, ID number, password, electronic files, data, or e-mail without prior authorization; or allowing such use by others;
6. Using District computer technology and communications resources in any unlawful manner including fraudulent, threatening, libelous, obscene, or harassing communications; procuring, or distributing obscene or pornographic material;
7. Circumventing or attempting to circumvent local, network, or remote security measures;
8. Altering or attempting to alter system software;
9. Altering or attempting to alter system hardware without Computer Services approval;
10. Modifying or attempting to crash or hack into computer technology or communications resources;
11. Accessing or attempting to access restricted portions of any operating system or security software unless authorized to do so;
12. Installing or removing software unless authorized to do so;
13. Using computer technology and/or communications resources for private commercial or other personal purposes;
14. Copying software that has not been placed in the public domain and distributed as freeware; inspecting, changing, altering, copying, or distributing proprietary data programs, files, disks, or software without authorization;
15. Falsely identifying and/or representing one's self in the use of computer technology and communications resources.

The District may access, review, copy and disclose information entered or retained in computer technology and communications resources.

Approved: 12/12/01