



SUNY Orange Policy Manual

Policy Number	Policy Title
BP2.8	Network and PC Utilization

The College computer network exists to enrich the learning environment and to enhance the effectiveness and efficiency of all other College operations. Usage of the network is a privilege and is limited to those functions.

Computers and networks are College property. The College reserves the right to access computer systems, including monitoring on-line activity and inspecting computer work areas. The reasons for which the College may obtain such access include, but are not limited to: maintaining the system, preventing or investigating allegations of system abuse or misuse; assuring compliance with software copyright laws; complying with legal and regulatory requests for information; and insuring that College operations continue appropriately during an employee's absence.

College policies regarding Sexual Harassment and Discrimination (**BP3.2**) and Harassment and Discrimination (**BP3.3**), in their entirety, apply to the use of College computers and networks. No one may use College computers or the network in a manner that may be construed by others as harassment or offensive based on age, race, marital status, veteran/military status, sexual orientation, religion, sex, national origin, ancestry, ethnicity, alienage, citizenship status, color, creed, handicap, disability, familial status and/or any other characteristics protected under applicable law.

The following are examples of prohibited uses:

- Displaying or transmitting material that is not educational or does not support the curriculum of the College and that could otherwise be considered sexually explicit, profane, racist, harassing, threatening or creating an intimidating, hostile or offensive environment
- Disguising the source of electronic messages by modifying the network in any way (includes adding access points or installing bridges, switches, hubs or repeaters)
- Running unauthorized programs or applications on the network
- Gaining unauthorized access to any electronic resource
- Circumventing security systems designed to prevent unauthorized access
- Accessing, downloading or storing of copyrighted software or information which is not licensed
- Transmitting any material in violation of United States or New York State law or regulations
- Using computing resources for commercial or profit-making activities; accessing or attempting to access any electronic resource for which the user does not have authorization
- Disrupting another user's work or system
- Broadcasting messages or any other activity that results in the congestion of the network distribution
- Sharing of user accounts and passwords

The College is responsible for the design, maintenance and good working order of the network and for providing ongoing user training on the appropriate uses of the network. The College is also responsible for investigating any suspected abuse of this policy. Such investigation may include remote monitoring of on-line activities and inspection of a user's computer work areas. If an abuse becomes apparent, the College may invoke stricter supervision, limit or revoke the user's privileges, or take other appropriate action, including discipline of College employees.

The Board of Trustees directs the President to develop such procedures as to fairly implement this policy.