Procedures Regarding Misuse of Computer Information AP 3250

This administrative procedure implements Board Policy 3250.

Abuse of computing, networking or information resources contained in or part of the District Network may result in the loss of computing privileges. Additionally, abuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable District or college policies, procedures, or collective bargaining agreements. Complaints alleging abuse of the District Network will be directed to those responsible for taking appropriate disciplinary action. Illegal reproduction of material protected by U.S. Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment.

Examples of behaviors constituting abuse which violate District Board Policy 3250 include, but are not limited to, the following activities:

System abuse

- Using a computer account that one is not authorized to use.
- Obtaining a password for a computer account that one is not authorized to have.
- Using the District Network to gain unauthorized access to any computer systems.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses and worms.
- Knowingly or carelessly allowing someone else to use your account who engages in any misuse in violation of Board Policy 3250 or of this AP 3250.
- Forging e-mail messages.
- Attempting to circumvent data protection schemes or uncover or exploit security loopholes.
- Masking the identity of an account or machine.
- Deliberately wasting computing resources.
- Downloading, displaying, uploading or transmitting obscenity or pornography, as legally defined.
- Attempting without District authorization to monitor or tamper with another user's electronic communications, or changing, or deleting another user's files or software without the explicit agreement of the owner, or any activity which is illegal under California Computer Crime Laws.
- Personal use which is excessive or interferes with the user's or others' performance of job duties, or otherwise burdens the intended use of the Network.
- Illegal downloading and/or distribution of copyright-protected materials, including but not limited to music and videos.

Harassment

- Using the telephone, e-mail or voice mail to harass or threaten others.
- Knowingly downloading, displaying or transmitting by use of the District Network, communications, pictures, drawings or depictions that contain ethnic slurs, racial epithets, or anything that may be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political belief.
- Knowingly downloading, displaying or transmitting by use of the District Network sexually explicit images, messages, pictures, or cartoons when done to harass or for the purposes of harassment.
- Knowingly downloading, displaying or transmitting by use of the District Network sexually harassing images or text in a public computer facility, or location that can potentially be in view of other individuals.
- Posting on electronic bulletin boards material that violates existing laws or the colleges' Codes of Conduct.
- Using the District Network to publish false or defamatory information about another person.

Commercial use

- Using the District Network for any commercial activity, without written authorization from the District. "Commercial activity" means for financial remuneration or designed to lead to financial remuneration.

Copyright

- Violating terms of applicable software licensing agreements or copyright laws.
- Publishing copyrighted material without the consent of the owner on District Web sites in violation of copyright laws.

Exceptions

Activities by technical staff, as authorized by appropriate District or college officials, to take action for security, enforcement, technical support, troubleshooting or performance testing purposes will not be considered abuse of the Network.

Although personal use is not an intended use, the District recognizes that the Network will be used for incidental personal activities and will take no disciplinary action provided that such use is within reason and provided that such usage is ordinarily on an employee's own time; is occasional and does not interfere with or burden the District's operation. Likewise, the District will not purposefully surveil or punish reasonable use of the network for union business-related communication between employees and their unions.

Complaints

A user who asserts that the District or District personnel have violated this policy shall file a complaint with his or her immediate supervisor with a copy to the Vice Chancellor of Human Resources, and a copy to the employee's bargaining unit. The supervisor shall notify the supervisor of the alleged violator to discuss the complaint. The supervisor of the complainant shall initiate an investigation if necessary and determine an appropriate remedy/resolution in consultation with the Vice Chancellor of Human Resources. In cases where the supervisor is part of the complaint, the complaint shall be filed with the next level of supervision for investigation and resolution and/or remedy. The complainant shall be informed in writing 1) of the initiation of the investigation, and 2) of its outcome as appropriate, with copies to the Vice Chancellor of Human Resources and the employee's bargaining unit. Complainants dissatisfied with the resolution/remedy have full recourse to relevant contractual protections and/or legal action.

Approved 11/17/97
Reviewed 8/16/99, 7/7/03
Revised 10/28/05, 2/6/09