ADMINISTRATIVE REGULATION 3720

SOUTH ORANGE COUNTY COMMUNITY COLLEGE DISTRICT

GENERAL INSTITUTION

ELECTRONIC COMMUNICATIONS

This administrative regulation is intended to inform all users (employees, contracted workers, students, and guests) of the District of the rules regarding use of the District's digital information network. The digital information network consists of District equipment such as computers, computer networks, electronic mail and voice mail systems, internet services, wireless networks, audio and video classroom and conferencing, and related electronic peripherals like cellular telephones, modems, and facsimile machines.

The information network is owned by the District and is to be used for District-related activities only. If District employees, students, or guests interface personally-owned equipment with the District network, they will be required to adhere to District policies and regulations.

I. PERMITTED USES OF THE DISTRICT'S DIGITAL INFORMATION NETWORK

Use of the digital information network is intended to enhance the availability of educational and work-related materials and opportunities for employees, students, and guests. Therefore, students and employees may only use the network for educational and work-related purposes. Guests in the Saddleback and Irvine Valley College Libraries may use the system on a limited basis with specific prior authorization from library staff and for educational and/or work-related purposes only. A guest network is available for one time use per semester for a max duration of eight hours. Community users must present identification to library staff for authorization and guest usage must not preclude student use.

A. Students are permitted access through workstations provided by the District at multiple locations, including all campuses, and in classroom/laboratory environments. Guests are provided kiosks or workstations for the sole purpose of applying and enrolling in courses. Community users can apply to receive access to Library computers located only in Library spaces for up to 30-day increments.

1. An electronic verification (signature) to acknowledge this regulation will be required at each login.

B. Employees are provided access through the above, or through assigned District computers.

1. An electronic verification (signature) to acknowledge this regulation will be required at each login.

C. Connection of privately owned equipment to campus wireless networks is permitted.

1. An electronic verification (signature) to acknowledge this regulation will be required at each login.

D. Connection of privately owned equipment to the network by physical (cable) is permitted when authorized by an administrator of one of the technology organizations at the colleges or the District to ensure compatibility of equipment.

Such authorizations will be in written form issued by a systems administrator indicating the person(s) is/are authorized to use personal equipment, and other relevant network information assigned to the equipment in order to enable use on the network.

II. USER RESPONSIBILITIES

Users shall not access information contained in restricted databases, files, and information banks, without permission from authorized District or college technology staff.

Personal passwords/account codes will be created and issued to users to protect employees and students. Users agree to represent themselves according to their true and accurate identities in all electronic messages, files, and transactions. These passwords/account codes shall not be shared with others, nor shall employees or students use another party's password/account code except in the authorized maintenance and monitoring of the network. The maintenance of strict control of passwords and account codes protects employees and students from wrongful accusation of misuse of electronic resources. If a communication is authored out of a password-protected system, the presumption will be that the owner of the password authored it.

Users have no right to privacy in any material on the network and/or e-mail system. The District reserves the right to monitor network and e-mail use for any business reason, including for the purpose of determining whether a violation of Board policy, administrative regulation, or law has occurred, and reserves the right to remove any materials or information found to be in violation of Board policy, administrative regulation, or law. Any monitoring will first be reviewed and approved by the Vice Chancellor of Educational and Technology Services and the Vice Chancellor of Human Resources. In addition, the District must perform necessary maintenance of the digital information network, which may also require access to information in user files, or files in the system which contains personal data.

III. PROHIBITED USES

Use of the digital information network is a privilege and not a right of any employee, guest, or student member, and that privilege may be modified or revoked at any time by the District for violation of District policy, administrative regulations, or any violation of law. The Vice Chancellor of Educational and Technology Services and/or the Vice Chancellor of Human Resources, applicable academic administrator, or designee shall take action with regard to any activity by users that is inconsistent with the permitted uses under this regulation and/or Board policy. Such action may result in revocation of user privileges and also lead to additional action being taken by the District as deemed necessary and appropriate. Prohibited uses include, but are not limited to, the following:

A. Communicating any information concerning any password, user account, personal identification number or confidential information protected by law without the permission of its owner or the controlling authority of the computer facility to which it belongs.

B. Forgery of messages and/or alteration of system and/or user data used to identify the sender of messages (includes sending anonymous messages).

C. Using District communication systems to solicit or conduct non-work related business.

D. Fundraising of any kind, except fundraising by faculty or staff that is work related.

E. Retrieving, viewing, or disseminating any material in violation of any federal or state regulation or District policy. This can include, but is not limited to, improper use of copyrighted material and improper use of passwords or access codes.

F. Damage, theft, or alteration of system hardware or software.

G. Disconnecting or otherwise tampering with District computers or network equipment and connections.

H. Connecting privately owned computers or other network capable devices to the network without appropriate authorization as specified from the system administrator.

I. Using any device to monitor, discover, or otherwise ascertain information regarding network operations not intended for public knowledge or consumption.

J. Placement of unlawful information, computer viruses, or harmful programs on or through the computer system.

K. Entry into restricted information on systems or network files in violation of password/account code restrictions.

L. Interfering with the abilities of others to use the District's systems.

M. Displaying images or audio that is obscene, sexually harassing, or otherwise violates the District rules prohibiting harassment.

N. Violating any laws, including but not limited to, copyright laws or laws regarding obscenity, or participating in the commission or furtherance of any crime or unlawful activity.

O. Sending unsolicited email, using social media platforms, streaming audio, streaming video, or playing multi-player games are not allowed, with the exception of those that serve educational or work-related purposes since they impose a substantial burden on the system.

P. For Students - Use of the network in furtherance of any violation of the Student Code of Conduct.

Q. For Employees - Use of the network in furtherance of any violation of applicable District policies or administrative regulations.

R. Employees or students may not use copyrighted materials without the permission of the copyright holder. The connections represented by the Internet allow users to access a wide variety of media. Even though it is possible to download most of these materials, users shall not create or maintain archived copies of these materials unless the materials are in the public domain.

S. Employees or students may not reverse engineer copyrighted materials or programs without the permission of the copyright holder.

T. District information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws.

U. Release of any individual's (student or employee) personal information to anyone without proper authorization.

IV. INCIDENTAL PERSONAL USE

Users of a District electronic communications system may use the system for incidental personal purposes for short periods of time, usually consisting of a few minutes per day, provided that such use does not:

A. directly or indirectly interfere with the District's operation of electronic communications resources;

B. interfere with the user's employment, duties, or other obligations of the District;

C. burden the District with incremental costs; or

D. violate any of the prohibited uses described in Section III.

The District is not responsible for any loss or damage incurred by an individual as a result of personal use of District electronic communications resources.

V. NONDISCRIMINATION

All users have the right to be free from any conduct connected with the use of the District network and computer resources which discriminates against any person on the basis of Administrative Regulation 3430 *Unlawful Harassment and Discrimination Prevention and Complaints*. No user shall use the District network and computer resources to transmit any message, create any communication of any kind, or store information which violates any District regulation regarding discrimination or harassment, or which is defamatory or obscene, or which constitutes the unauthorized release of confidential information.

VI. ENFORCING THIS REGULATION

Due to the open and decentralized design of the internet and the digital information network, the District cannot protect individuals against receipt of material that may be offensive to them. Likewise, individuals who use email, or those who disclose private information about themselves on the internet or across the digital information network, should know that the District cannot protect them from invasions of privacy by third parties or other users.

The Vice President of Student Services will determine violations by students, the Vice Chancellor of Human Resources in consultation with the Vice Chancellor of Educational and Technology Services will determine violations by employees and/or contractors, the administrator of Library and Learning Resources will determine violations by guests. These administrators may, with the approval of the Chancellor, name designees who will perform these functions.

District employees and other users may informally resolve unintentional or isolated minor violations of use policies.

A. Employee Violations - Individuals may report a suspected violation of this regulation or Board policy by employees and/or contractors to their supervisor. In turn, the supervisor will notify the Vice Chancellor of Human Resources. The Vice Chancellor of Human Resources in consultation with the Vice Chancellor of Educational and Technology Services shall then determine whether a violation of this regulation or Board policy has occurred. If it is determined that a violation has occurred, the Vice Chancellor of Human Resources may take immediate action to suspend or revoke the user's privileges, provide the user with written notice of the suspension or revocation, and provide a statement of reasons for the action taken. The Vice Chancellor of Human Resources will make a determination of whether disciplinary action should be taken pursuant to established District collective bargaining agreements, Board policies, administrative regulations, and/or other applicable laws, rules, or procedures.

B. Guest Violations - Individuals may report a suspected violation of this regulation or Board policy by a guest to the supervisor of the library/laboratory. In turn, the library/laboratory supervisor will notify the administrator of Library and Learning Resources or designee. The administrator shall then determine whether a violation of this regulation or Board policy has occurred. If the administrator determines that a violation has occurred, the administrator may take immediate action to suspend or revoke the user's privileges. In the event a user's privileges are suspended or revoked, the administrator will provide the user with written notice of the suspension or revocation and provide a statement of reasons for the action taken. If requested by the user, the administrator will meet with the user within five business days. The administrator may also submit the matter to the college president for a determination of whether additional action should be taken. Possible sanctions include the deletion of the materials found to be in violation of this regulation or Board policy, loss of user privileges, and other sanctions available within the judicial processes.

References:

Education Code Section 70902
Government Code Section 3543.1(b)
Penal Code Section 502
17 U.S. Code Sections 101 et. seq.