

ELECTRONIC COMMUNICATIONS

This administrative regulation is intended to inform all users (faculty, staff, and students) of the South Orange County Community College District of the rules regarding responsible use of the District's digital information network. The digital information network consists of District owned equipment such as computers, computer networks, electronic mail and voice mail systems, internet services, audio and video conferencing, and related electronic peripherals like cellular telephones, modems and facsimile machines.

The digital information network is owned by the District and is to be used for District-related activities only. If District faculty, staff, or students bring personally-owned equipment into the District environment, they will be required to adhere to District policies and regulations when such equipment is used in conjunction with District owned equipment.

The District recognizes the important role access to electronic information and the internet play in modern research and education. However, the District also recognizes that responsible use of these technologies is important to maintain an appropriate educational environment and to ensure that District resources are provided to all on an equal basis.

I. Permitted Uses of the District's Digital Information Network

Use of the digital information network is intended to enhance the availability of educational materials and opportunities for faculty, staff, and students. Therefore, use of this network is limited to activities which are reasonably related to the educational goals of the District. While the District encourages broad and extensive use of the network for educational and work-related purposes, personal, recreational, or commercial use of the system by faculty, staff, and students for non-academic matters is not permitted.

1. Guests and students are permitted access through open workstations provided by the District at multiple locations, including both campuses, and in classroom/ laboratory environments.
  - a. An electronic verification (signature) to acknowledge this policy will be required at each log-in.
2. Faculty and Staff are provided access through the above, or assigned District-owned computers.
  - a. An electronic verification (signature) to acknowledge this policy will be required at each log-in.

3. Connection of privately owned computer equipment to the network by physical (cable) or wireless means is permitted when authorized by the appropriate administrator of one of the technology organizations at the colleges or the District.
  - a. Such authorizations will be in written form issued by a systems administrator indicating the person(s) authorized to use personal equipment, and other relevant network information assigned to the equipment in order to enable use on the network.

Use of the digital information network is a privilege and not a right of any faculty, staff, or student member, and that privilege may be modified or revoked at any time by the District for violation of District policy or administrative regulations, or any violation of law.

## II. Personal Responsibility

Use of the District's digital information network requires that users take personal responsibility for appropriate use of this technology. Users must remember that information distributed on the Network reflects upon the image of the District and not just the individual, and so appropriate decorum and etiquette is required. Users shall respect that some areas of information are contained in restricted data bases, files, and information banks, and are consequently unavailable. Users shall not access such information without appropriate permission.

Personal passwords/account codes will be created and issued to users to protect faculty, staff, 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 faculty, staff, 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 faculty, staff, 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. Faculty, staff, or students who misuse electronic resources or who violate laws will be disciplined at a level appropriate to the seriousness of the misuse and may have their user privileges revoked by the District.

Access to electronic mail (e-mail) is a privilege and designed to assist users in the acquisition of knowledge and in efficiently communicating with others. The District e-mail system is designed solely for educational and work-related purposes. Users must remember that the District does not provide a right to privacy in any material on the network and/or the use of its e-mail system. The District reserves the right to monitor Network and e-mail use for the purpose of determining whether a violation of District policy, administrative regulation, or other law has occurred, and reserves the right to remove any such information.

Chain letters, “chat rooms,” Multiple User Dimensions (MUDs), or multi-player game servers are not allowed, with the exception of those bulletin boards or “chat” groups that are created by academic staff for specific instructional purposes or employees for specific work-related communication.

### III. Prohibited Uses

The use of the District’s digital information network is a privilege which may be revoked at any time for violation of acceptable use or actions which jeopardize the network’s infrastructure, design or intended connections or access, and use by others. While it is not practical to comprehensively list all prohibited uses of the network, and without intending to discourage positive, constructive, and open use of the network, the general provision that shall be in force to define prohibited used actions or activities on the network is: “That which is not expressly permitted is denied.”

In keeping with that provision, authority is vested with the system administrator(s) to take whatever action is necessary and appropriate to stop any activity by users which is inconsistent with the permitted uses under this regulation and/or board policy.

Behaviors which will result in revocation of user privileges and may result in additional action being taken by the District as necessary and appropriate include, but are not limited to, the following:

1. Communicating any information concerning any password, user account, personal identification number or other confidential information without the permission of its owner or the controlling authority of the computer facility to which it belongs.
2. Forgery of messages and/or alteration of system and/or user data used to identify the sender of messages.
3. Using District communication systems to solicit or conduct business other than the business of the District.
4. Soliciting or advocating for issues, causes, or organizations of any kind when such solicitation or advocacy is deemed personal in nature and not recognized as furthering the reputation and interests of the District.
5. Unauthorized fundraising of any kind.
6. Personal use of the District communication systems that preempts any business activity or interferes with productivity.
7. Retrieving, viewing, or disseminating any material in violation of any federal or state regulation or District policy. This includes, but is not limited to, improper use of copyrighted material and improper use of passwords or access codes.

8. Downloading or disseminating copyrighted or other proprietary material, other than downloading such material for personal use only.
9. Damage, theft, or alteration of system hardware or software.
10. Disconnecting or otherwise tampering with District owned computers or network equipment and connections.
11. Connecting privately owned computers or other network capable devices to the network without appropriate authorization as specified from the system administrator.
12. Using any device to monitor, discover, or otherwise ascertain (i.e. “sniffing” or “hacking”) information regarding network operations not intended for public knowledge or consumption.
13. Placement of unlawful information, computer viruses, or harmful programs on, or through the computer system.
14. Entry into restricted information on systems or network files in violation of password/account code restrictions.
15. Disrupting the educational process, or interfering with the rights of others to use the District’s systems.
16. Viewing, transmitting, or otherwise engaging in any communication which contains obscene, indecent, profane, lewd, or lascivious material or other material which explicitly or implicitly refers to sexual conduct.
17. Displaying sexually explicit or sexually harassing images or text in a private and/or public computer facility or location that can potentially be in view of other individuals.
18. Use of the network for personal gain, commercial purposes, or to engage in political activity.
19. Violating any laws or participating in the commission or furtherance of any crime or other unlawful or improper purpose.
20. (For Students) Use of the network in furtherance of any violation of the Student Code of Conduct.
21. (For Faculty and Staff) Use of the network in furtherance of any violation of applicable collective bargaining agreements, District policies or administrative regulations.

Users may not claim personal copyright privileges over files, data, or materials developed in the scope of their employment, nor may faculty, staff, or students 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, e.g., freeware, shareware, etc.

#### IV. Investigating Violations of 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.

All users shall report known violations of this administrative regulation to the District. Reported violations will be investigated as deemed appropriate by the District. Although the District intends to respect user's privacy to the extent possible, there are circumstances which will require the District to retrieve information concerning use of the digital information network to detect violations and determine the responsible party or parties. 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.

District faculty, staff, and students may informally resolve unintentional or isolated minor violations of use policies through email or face-to-face discussion and education with the user or users concerned.

##### 1. Student Violations

Individuals may report a suspected violation of this regulation or board policy by a student to the supervisor of the library/laboratory. In turn, the library/laboratory supervisor will contact the Dean of Technology for appropriate processing. The Dean shall determine whether a violation of this regulation or of board policy has occurred. If the system administrator determines that a violation has occurred, the Dean may take immediate action to suspend or revoke the user's privileges in addition to other remedial actions which are deemed appropriate. In the event a user's privileges are suspended or revoked, the Dean will provide the user with written notice of the suspension or revocation, and provide a statement of reasons for the actions taken. Thereafter, the Dean may also submit the matter to the appropriate District department for a determination of whether additional action should be taken. Possible sanctions include the deletion of materials found to be in violation of this regulation or of board policy, loss of user privileges, student discipline, and other sanctions available within the judicial processes.

2. Faculty and Staff Violations

Individuals may report a suspected violation of this regulation or board policy by District employees to their supervisor. In turn, the supervisor will notify the appropriate technology administrator (Dean of Technology for college staff, Director of Information Technology for District Services staff) for appropriate processing. 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. The administrator may also submit the matter to the appropriate academic or classified staff supervisor or administrator for a determination of whether disciplinary action should be taken pursuant to established District collective bargaining agreements, District policies, administrative regulations, and/or other applicable laws, rules, or procedures.

3. Guest Violation

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 Dean of Technology for appropriate processing. The Dean shall then determine whether a violation of this regulation or of board policy has occurred. If the Dean determines that a violation has occurred, the Dean may take immediate action to suspend or revoke the user's privileges. In the event a user's privileges are suspended or revoked, the Dean will provide the user with written notice of the suspension or revocation, and provide a statement of reasons for the action taken. The Dean 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.