ACCEPTABLE USE POLICY
INTERNET AND OTHER COMPUTER NETWORKS

The Southwestern Community College District ("District") promotes the use of Internet resources for purposes consistent with the educational mission and curriculum. The District's goal is to promote the free exchange of information between and among currently enrolled students, faculty, staff, and the global information community. The District provides access to local, national and international sources of information and provides an atmosphere that encourages access to knowledge and sharing of information. Responsible use of this access includes:

- Respect for the privacy of others; for example, users shall not seek information on, obtain copies of, or modify files, other data or passwords belonging to other users unless explicitly authorized to do so by those users.

- Respect for the legal protection of copyright and license agreements for programs and data.

- Respect for the integrity of computing systems; for example, users shall not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software or hardware components of a computer or computing system.

District computer systems facilitate access to and distribution of information. The District has no editorial control over the content, materials or data distributed or disseminated on the network. The quality and content of the materials that exist on electronic data networks are beyond the control of the District. Users are responsible for the materials that they access through District resources.

POLICY REQUISITE

All users of computing systems must read, understand, and comply with the terms outlined in this Policy, as well as any additional guidelines established by District computer systems administrators. By using any of these systems, users agree that they will comply with these policies. Users understand and agree that the District's role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of said transmission by the District.

RIGHTS

These computer systems, facilities and accounts are owned and operated by the District. The District reserves all rights, including termination of service without notice, to the computing resources which it owns and operates. This policy shall not be construed as a waiver of any rights of the District, nor shall they conflict with applicable law.

AUTHORIZED USE

Access and privileges on the District's computing systems are assigned and managed by the administrators of the specific individual systems. Eligible individuals may become authorized users of the system and be granted appropriate access and privileges by following the approval steps prescribed for that system.

All access to the District's computer resources, including issuing of passwords, must be approved by an authorized District agent.

GENERAL ACCEPTABLE USES OF THE NETWORK

- Scholarship, scientific research, or instructional applications engaged in by students, faculty and staff.
- Communication and exchange for professional development, to maintain currency, or to debate issues in a field or sub-field of knowledge.
- Discipline-society, college-association, government-advisory, or standards activities related to user's research, instructional and administrative activities.
- Access to college and university libraries and information and news from a variety of sources and research institutions.
- Access to information resources, computers and people throughout the world.
- Interaction with students, faculty and staff by electronic mail.
- Discussion groups on a wide variety of topics.
- Administrative activities which are part of the support infrastructure needed for instruction, scholarship, student services and institutional management.

UNACCEPTABLE USES OF THE NETWORK

Use of any and all of the District's computer systems for any of the purposes listed in this section is strictly prohibited. Liability for violations of prohibited uses shall remain solely and exclusively with the user. By using the District's computer systems, the user further agrees to indemnify the District for any liability incurred by the District for misuse by the user.

The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through the District's system.

The user agrees that, in the event that someone does transmit, or cause to be transmitted, a message, information or material of any kind that is inconsistent with an environment conducive to learning or conducting college business or with a misleading origin, the person who performed the transmission will be solely accountable for the message, not the District, which is acting solely as the information carrier.

District computer accounts and/or equipment may not be used for the following purposes:

1. **Illegal Activity**: Any illegal use of the network, or its use in support of such activities, is strictly prohibited. Illegal activities shall be defined as a violation of local, state, and/or federal laws. Criminal activities include:

    a. Hacking/Computer Vandalism. Activities which interfere with or disrupt network users, services or equipment are prohibited. Such interference or disruption includes, but is not limited to:

        1. Distribution of unsolicited advertising or mass mailings;

        2. Propagation of computer worms or viruses; and

        3. Using the network to make or attempt to make unauthorized entry to other computational, information or communications devices or resources or to other users' files.

    Intentional interception of any electronic communication is considered improper access and may also be in violation of the Electronic Communications Privacy Act, Chapter 119. The submission, publication or transmission of information for the purpose of inciting crime is strictly prohibited.

    Unauthorized reconfiguration of or physical tampering with District resources is not allowed. Users must not attempt unauthorized modification or repair to any equipment belonging to or under the control of the District.

b. Violation of Software Licenses. The District licenses the use of its computer software from a variety of companies. The District does not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it. Users must not violate the license agreements on any software applications installed on a District computer. Use of District computing facilities for private business activities or other non-educational functions violates the software license agreements extended to educational institutions and is not permitted.

- It is District policy that employees, students and other users of District computing facilities shall use the software only in accordance with the license agreement.

- District employees, students or other users found to be making, acquiring or using unauthorized copies of computer software will be disciplined as appropriate under the circumstances.

c. Violation of Copyrights. Information and resources accessible via District computer accounts are the private property of the individuals and organizations who own or hold rights to the resources and information. Users must not access information or resources unless permission to do so has been granted by the owners of rights to those resources or information. Users must not submit, publish, plagiarize, or transmit material which violates or infringes upon the copyrights held by others.

2. **Inappropriate Use**: Any inappropriate use of the network, or its use in support of such activities, is prohibited. Inappropriate use shall be defined as a violation of the goals, purposes and intended use of the network. District computing resources may not be used for political campaigns. Users must not use the District network access to create, publish, display, or transmit any materials that are threatening, defamatory, fraudulent, seditious, abusive, obscene, profane, or sexually oriented. Repeated transmission of material to a person who finds such transmission offensive, obscene or discriminatory will be treated as harassment and is against District policy and State and Federal regulations.

   Users agree not to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading.

3. **Commercial/For Profit Activity**: Any commercial, for-profit activity including marketing, sales, and distribution of mass mailings is prohibited. Users may not use the District network to make private purchases or transfer personal funds.

4. **Extensive Personal Use**: Extensive use of the District's network access for personal business is prohibited.

Unauthorized access, attempted access or use of any District computer or computer network system is a violation of Section 502 of the California Penal Code and/or other applicable Federal laws, and is subject to prosecution. The District reserves the right to prosecute any unlawful access or injury to any computer, computer system, computer network, computer program, or data to which the District provides access and or/services.

Any student or staff member who uses District resources illegally or improperly may be subject to disciplinary actions, revocation of access to the District network, and possible legal action. The District will review alleged violations of the Acceptable Use Policy on a case-by-case basis. Failure to abide by these guidelines will result in revocation of privileges to use the computer systems. Students may also be subject to disciplinary sanctions up to and including dismissal from the institution. Staff members will be subject to appropriate disciplinary action.

ACCOUNT AND SYSTEM SECURITY

Each individual user is responsible for the proper use of their assigned account, including password protection. Users must not share their computer account with others who have not received District authorization. In the event of disciplinary action, the fact that someone else used your account will be no excuse for violations of this Acceptable Use Policy. User accounts assigned to another person must not be used without written permission of the system administrator.

District personnel responsible for the care, operation, use and maintenance of computing systems will make every reasonable effort to minimize the loss of data in their efforts to maintain privacy and security on the systems. However, the District is not responsible for the loss of data or interference with files resulting from its efforts to maintain the District's computer facilities.

Users should save their data files to their own disks. The District is not responsible for lost or deleted files that have been saved onto District disks. The District is not responsible for disk or file damage due to viruses. Users are advised not to reveal the address, phone number, or other personal details about themselves or others.

SYSTEM MAINTENANCE AND MONITORING

Computer files, electronic mail and accounts on District computing systems are not the private property of the user. Users should have no reasonable expectations of privacy. Authorized District personnel may access others' files when necessary for the maintenance or protection of the computing facilities and to conduct college business. When maintenance is being performed, every effort will be made to ensure the privacy of users' files. However, in the course of network maintenance and administration, the activities of individuals improperly using the network may be monitored. Individuals using the network without authority, or in excess of their

authority, are subject to having all of their activities on the network monitored and recorded. Anyone using the network expressly consents to such monitoring and is advised that, if such monitoring reveals possible evidence of criminal activity, the District may provide the content of such monitoring to law enforcement and national defense agencies as appropriate.