Southwest Mississippi Community College Network Acceptable Use Policy

Revised: 2 March 2011

I. Summary/Purpose

The purpose of the SMCC network is to provide faculty, staff, and students with an electronic means of transmitting, receiving, and reviewing information necessary for academic pursuits as well as conducting daily business operations of the college. The Acceptable Use Policy covers all devices that comprise the SMCC network. This includes, but is not limited to, all desktop systems, hand-held computers, lab facilities, servers, laptops, classroom technology, the wired and wireless campus networks, and all software licensed to the college.

II. Rights and Responsibilities

The SMCC network is provided and maintained by the SMCC IT department for the use of faculty, staff, and students. Accounts are created and given to all users for the purpose of academics, transmitting and receiving electronic mail and messages, daily business and administrative operations, and other authorized activities. Anyone using the SMCC network is responsible for:

- recognizing and honoring the intellectual property rights of others, making attribution as appropriate;

- refraining from any illegal and improper intrusions into the accounts of others or into any SMCC network resources or systems;

- taking all reasonable steps to insure the accuracy and the security of information compiled, accessed, or provided;

- being ethical and respectful of the rights of others and of the diversity of the college community, including the rights to privacy and all other legal requirements and restrictions regarding access to and use of information; and refraining from acts that waste resources and prevent others from having broad access to SMCC IT resources;

- abiding by all other applicable college policies and standards relating to information technology resources. These policies and standards include, but are not limited to: software, wireless, remote access and email.

Users are responsible for all activities to and from their network accounts. Users must take every precaution to protect logins and passwords. Under no circumstances should a user allow someone else to share a network or e-mail account.

III. Consent to Monitor

SMCC's computers and networks are shared resources, for use by all faculty, staff, and students. Any activity that inhibits or interferes with the use of these resources by others is not permitted. The college will ensure reasonable use by monitoring access logs, traffic data, and network utilization. By logging on to and using network resources, the user agrees to the SMCC Acceptable Use policy and the SMCC Consent to Monitor section of said policy. **SMCC can examine, at any time, anything that is stored on or transmitted by college-owned equipment.** This includes, but is not limited to, e-mail, data files, software, websites, and stored documents. Users should not assume or expect any right of privacy with respect to the SMCC network resources. Although the college does not seek to monitor the communication of its faculty, staff, or students, SMCC IT staff may access or examine files or accounts that are suspected of unauthorized use or misuse, that have been corrupted or damaged, or that may threaten the integrity of SMCC's computer systems. In addition, files, e-mail, access logs, and any other electronic records may be subject to search under court order.

IV. E-Mail Usage

SMCC recognizes the utilization of electronic communications as an efficient and necessary method of conducting business and advancing its mission of education. Electronic mail (e-mail) should be used with the same care and discretion as any other type of official college communication.

The SMCC e-mail system is not a private secure communications medium. As such, e-mail users cannot expect privacy. By using the SMCC e-mail system, each user acknowledges:

- The use of electronic mail is a privilege not a right. E-mail is for college communication, research, or campus business. Transmitting certain types of communications is expressly forbidden. This includes messages containing chain letters, pyramids, urban legends, and alarming hoaxes; vulgar, obscene or sexually explicit language; threatening or offensive content; derogatory, defamatory, sexual, or other harassment; and discriminatory communication of any kind. As with other information technology resources, the use of e-mail for commercial or political purposes is strictly prohibited.

- Under the Electronic Communications Privacy Act, tampering with e-mail, interfering with the delivery of e-mail, and using e-mail for criminal purposes may be felony offenses, requiring the disclosure of messages to law enforcement or other third parties without notification.

- E-mail messages should be transmitted only to those individuals who have a need to receive them. Distribution lists should be constructed and used carefully. E-mail distribution lists should be kept current and updated regularly. Inappropriate mass mailing is forbidden. This includes multiple mailings to newsgroups, mailing lists, or individuals (e.g. "spamming," "flooding," or "bombing").

- All users of the SMCC e-mail system waive any right to privacy in e-mail messages and consent to the access and disclosure of e-mail messages by authorized college personnel.

Accordingly, the college reserves the right to access and disclose the contents of e-mail messages on a need-to-know basis. Users should recognize that under some circumstances, as a result of investigations, subpoenas, or lawsuits, the college might be required by law to disclose the contents of e-mail communications.

SMCC Confidentiality Agreement:

The information transmitted in this electronic mail is intended only for the person or entity to which it is addressed and may contain confidential, proprietary, and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from all computers. Southwest MS Community College (SMCC) accepts no liability for the content of this message or for the consequences on any actions taken on the basis of information provided, unless the information is subsequently confirmed in writing by an authorized representative of SMCC. Although SMCC has taken reasonable precautions to ensure that no viruses are present in this message, SMCC cannot accept responsibility for any loss or damage arising from the use of this message.

V. Privacy

SMCC provides computers, computer and e-mail accounts, networks and telephone systems to faculty members, staff and students for the purpose of furthering the college's academic mission and conducting business. While incidental and occasional personal use of such systems, including e-mail and voice mail, is permissible, personal communications and files transmitted over or stored on SMCC systems are not treated differently from business communications; there can be no guarantee that personal communications will remain private or confidential.

Section 25-65-17 of the Mississippi Code states that "internal audit staff shall have access to all personnel and any records, data and other information of the university, community/junior college or state agency deemed necessary to carry out assigned duties."

Those responsible for maintaining SMCC's computers and electronic networks have a responsibility to recognize when they may be dealing with sensitive or private information. They may access such information without the user's consent when necessary to fulfill their official responsibilities. Properly authorized individuals including the Director of Information Technology and the SMCC IT staff may access e-mail, voice mail or computer accounts without the consent of the assigned user when there is a reasonable basis to believe that such action:

- is necessary to comply with legal requirements or process, or

- may yield information necessary for the investigation of a suspected violation of law or regulations, or of a suspected serious infraction of policy (for example alleged misconduct, plagiarism or harassment), or

- is needed to maintain the integrity of SMCC computing systems, or

- may yield information needed to deal with an emergency, or

- in the case of staff, will yield information that is needed for the ordinary business of the college to proceed.

These individuals will be subject to disciplinary action if they misuse their access to personally identifiable data or to individuals' personal files, e-mail and voice mail or otherwise knowingly act in ways counter to SMCC policies and applicable laws.

VI. Unacceptable Usage

Some examples of violations of SMCC policy are given below. This is by no means a comprehensive list and other activities that are against SMCC policies are still considered violations of the Acceptable Use policy even if not specifically listed.

- Logging on or attempting to log on with a username other than one’s own.

- Logging on with an account and allowing others free usage of the computer while logged into the campus network.

- The sharing of music, video, or other copyrighted materials via Peer-to-Peer networking software (Kazaa, Morpheus, Bearshare, Grokster, etc.).

- Accessing any computing resource to which authorization has not been validly given.

- Connecting a personal computer/laptop to the SMCC network without authorization from the SMCC IT department.

- Performing any act which seriously impacts the operation of computers, peripheral devices, or the network, including tampering with the components of a local area network (LAN) or alterations of computer hardware which hampers the operational readiness of a computer.

- Knowingly installing unauthorized programs including, but not limited to, chat clients, MUD, MUSH, sniffers, Spyware, toolbars, and any other malicious program.

- Copying, installing or using any software or data files that violate a copyright or license agreement.

- Deliberately changing the contents of any e-mail header or TCP/IP data packet header to conceal one’s identity.

- Sending, receiving, sharing or storing mail, files, messages, etc. that contain:
  a. profanity, obscenities, or other language of an inflammatory nature;
  b. information which infringes upon the rights of another person;
  c. information which may injure someone else and/or lead to a lawsuit or

criminal charges;

d. information which consists of any advertisements for commercial enterprises;

e. files or information covered under the Digital Millennium Copyright Act (DMCA) unless permission has been obtained from the owner(s).

- Employing an internet browser (Internet Explorer, Firefox, Netscape, etc.) on a campus computer for the sole purpose of surfing the Internet in search of pornographic sites, illegal gambling sites, or other similar, questionable sites.

- Using computing resources for commercial activities and/or personal gain, for example, running an internet business from a campus computer.

- Any attempt to circumvent user authentication methods, data protection schemes, network security lockdown procedures, uncover security loopholes, exploit software vulnerabilities, or any attempt to probe or scan a system or network without explicit permission from the SMCC IT staff.

- Performing any act which is wasteful of computing resources, including, but not limited to, mass mailing (SPAM), chain letters, e-mail hoaxes, creating unnecessary output (both electronic or hard copy), or preventing the pursuit of academic research by tying up computing resources with online games or other unnecessary network traffic.

- Using computing and/or network resources to gain unauthorized access to remote computers; using computing and/or network resources to launch Denial of Service attacks, broadcast attacks, mail-bombing, packet-flooding or overloading any system located on or off the premises.

- Using computing resources to harass others by sending annoying, threatening, libelous, or sexually, racially, or religiously offensive messages.

- Using computing resources to monitor another user's data communications, or reading, copying, or deleting another user's files or software without permission of the owner.

- Using computer resources to develop, perform, and/or perpetuate any unlawful act or to improperly disclose confidential information.

VII. File Sharing and Copyright Infringement

Federal copyright law applies to all forms of information, including electronic communications. Members of the SMCC community should be aware that copyright infringement includes the unauthorized copying, displaying, and/or distributing of copyrighted material. All such works, including those available electronically, should be considered protected by copyright law unless specifically stated otherwise.

SMCC complies with all provisions of the Digital Millennium Copyright Act (DMCA). Any use of the SMCC network, e-mail system, or web site to transfer copyrighted material including, but not limited to, software, text, images, audio, and video is strictly prohibited. Therefore, the use of popular file sharing programs such as KaZaA, Morpheus, Azureus, FrostWire, LimeWire, BitTorrent, etc. are a violation of SMCC policy and federal law.

SMCC also maintains policies and procedures pursuant to the Higher Education Opportunity Act (HEOA). Under this law, SMCC has put into place "technology-based deterrents" to discourage illegal file sharing. These deterrents include but are not limited to:

- Bandwidth shaping
- Traffic monitoring to identify the largest bandwidth users
- A vigorous program of accepting and responding to Digital Millennium Copyright Act (DMCA) notices
- A variety of commercial products designed to reduce or block illegal file sharing

Anyone using SMCC network resources to commit acts of copyright infringement may be subject to prosecution. Acts of piracy are violations of state and federal laws, and as such, may result in criminal charges.

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.

VIII. Wireless Network Usage

SMCC provides wireless network access at various points around the campus. As such, these wireless networks are subject to the same policies and restrictions as wired networks.

Use of wireless networks constitutes an agreement by the student to abide by the SMCC Acceptable Use Policy. It is the policy of SMCC to forbid the use of any P2P or sharing software, “hacking” or proxy avoidance software, or any software designed to circumvent, damage, or remove any of the network security measures currently in place on the campus networks.

Users who violate this policy will have their computer blocked from accessing the wireless network for 7 days and will need to remove the software from their computer before being allowed to use the service again. A second violation will result in the user being barred from wireless access for 30 days. If the user violates the policy a third time, the individual computer will be permanently blocked from accessing the SMCC network.

IX. Private Computers Connected to the SMCC Network

The following apply to anyone connecting a private computer to the SMCC network, wireless LAN connection, or a regular network connection in an office or residence hall.

• The owner of the computer is responsible for the behavior of all users on the computer, and all network traffic to and from the computer, whether or not the owner knowingly generates the traffic.

• A private computer connected to the network may not be used to provide network access for anyone who is not authorized to use the college systems. The private computer may not be used as a router or bridge between the SMCC network and external networks, such as those of an Internet Service Provider.

• Should the SMCC IT staff have any reason to believe that a private computer connected to the SMCC network is using the resources inappropriately, network traffic to and from that computer will be monitored. If justified, the system will be disconnected from the network, and appropriate action will be taken.

• Any residential student, with an authorized network account, may use the SMCC network connection for scholarly purposes, for official college business, and for personal use, so long as the usage:
a. does not violate any law or this policy,
b. does not involve extraordinarily high utilization of college resources or substantially interfere with the performance of the SMCC network, and
c. does not result in commercial gain or profit.

• Due to the possibility of a breach in the college's computer network security, students are not permitted to connect a computer to the SMCC network and an external Internet Service Provider

AT THE SAME TIME. Students who prefer to use an external ISP must notify SMCC IT prior to connecting to the external ISP network.

• Users are responsible for the security and integrity of their systems. In cases where a computer is "hacked into," it is recommended that the system be either shut down or be removed from the campus network as soon as possible to localize any potential damage and to stop the attack from spreading. If you suspect electronic intrusion or hacking of your system and would like assistance, contact the SMCC IT department immediately.

• The following types of servers should never be connected to the SMCC network: DNS, DHCP, BOOTP, WINS, or any other server that manages network addresses.

X. Penalties

If a user is suspected of violating this Policy, SMCC may confiscate any equipment, device, software, documents, or data that is involved.

If an individual has violated the Policy, he/she will incur the same types of disciplinary measures as violations of other SMCC policies. Violation of state or federal free/statutes may lead to criminal or civil prosecution.

Students: Campus disciplinary measures may include, but are not limited to, failure in a class, permanent or temporary loss of information technology privileges, suspension or expulsion from SMCC, and restitution of expenses as well as charges for damages.

Faculty and Staff: Campus disciplinary measures may include, but are not limited to, reassignment of duties, transfer, censure, suspension, termination, and restitution of expenses as well as charges for damages.

Off-campus Users: The college may revoke the privileges of users who are found to be in violation and may report any serious violation to the users home campus authorities and to appropriate law enforcement officials.

XI. Mississippi Laws that Apply to Use of Computing and Networking Systems and to Publicly Accessible Web Pages

The following are examples of violations of the laws of the State of Mississippi (Mississippi Code of 1972 - http://www.mscode.com/free/statutes/97/045/0011.htm):

• Public display of sexually oriented materials in a venue likely to be visited by minors in the normal course of business.
(Reference: http://www.mscode.com/free/statutes/97/005/0029.htm)

• Intentional deceit of anyone as to an individual’s true identity for the purpose of obtaining anything of value. Users should not use each other’s e-mail accounts at all, but to do so for personal gain is illegal.
(Reference: http://www.mscode.com/free/statutes/97/019/0085.htm)

- Profane or indecent language in a public place. A web page which resides on a University server is a public place.
(Reference: http://www.mscode.com/free/statutes/97/029/0047.htm)

- Publishing or exhibiting obscene materials.
(Reference: http://www.mscode.com/free/statutes/97/029/0101.htm)

- Hacking or passing along hacker information concerning a computer, computer system, or network to another person. Obtaining services to which an individual is not entitled and either inserting or changing system files are all illegal.
(Reference: http://www.mscode.com/free/statutes/97/045/0003.htm)

- Blocking another user from using a system he/she is entitled to use.
(Reference: http://www.mscode.com/free/statutes/97/045/0005.htm)

- Using or sharing the results of cracking a password file. This may result in up to five years in jail and a fine of up to $10,000.
(Reference: http://www.mscode.com/free/statutes/97/045/0005.htm)

- Intentional modification or destruction of computer equipment or supplies.
(Reference: http://www.mscode.com/free/statutes/97/045/0007.htm)

- Erasing, modifying, sharing, or using the information in the files of another user.
(Reference: http://www.mscode.com/free/statutes/97/045/0009.htm)

- All of the activities outlined in the Mississippi Code are unlawful if the user was physically in Mississippi when the act was committed, was committing the act against a computer or system in Mississippi, or used a computer or network in Mississippi as a relay point.
(Reference: http://www.mscode.com/free/statutes/97/045/0011.htm)

XII. Indemnification/Liability Statement

Southwest Mississippi Community College makes absolutely no warranties of any kind, either express or implied, for the IT services it provides. The college will not be responsible for any damages suffered by users including, but not limited to, any loss of data resulting from delays, non-deliveries, user errors, or service interruptions.

The college is not responsible for the accuracy or quality of information obtained through its IT services, including e-mail. Users assume responsibility for any damages suffered as a result of information obtained through these sources.

The user agrees to indemnify and hold harmless Southwest Mississippi Community College, the Board of Directors, and college faculty, staff, and employees from and against any claim, lawsuit, cause of action, damage judgment, loss, expense, or liability resulting from any claim, including reasonable attorneys’ fees, arising out of or related to the use of the college's hardware, software, and network facilities.

This indemnity shall include, without limitation, those claims based on trademark or service mark infringement, copyright infringement, defamation, unlawful discrimination or harassment, rights of publicity, and invasion of privacy.