Acceptable Use Policy

The goal of participation in the Internet is to provide access for Southwestern Michigan College (henceforth, "SMC") students, alumni, faculty, staff and administration, which will facilitate far-reaching communication opportunities.

The intent of this policy is to comply with, and supplement, the stated purpose and acceptable use policies of any other networks utilized, the law of the State of Michigan and United States Copyright Laws. Acceptable use is not limited to this policy, as departments or divisions of the college may include additional stipulation.

This Acceptable Use Policy applies to all individuals (henceforth, "users" or "accounts") accessing equipment connected to the local/wide area network at SMC or on the Internet (henceforth, "the network"), both on-premises and remote connections through direct or dial-up means.

Purpose – Persons are granted access to the network to facilitate their studies, their instruction, the discharge of their duties as employees, their official business with the College, and other SMC-sanctioned activities. Additional opportunity exists for diversity awareness, personal and/or professional growth, and communication skills pertaining to 1) curriculum available through SMC instruction and consistent with student conduct policy, or 2) SMC Board of Trustees policy. The network shall aid in the development of mutual respect for the ideas and information of others.

Method of Access – The following applications may be used for accessing information: Electronic Mail (e-mail), Telnet, File Transfer Protocol (FTP), and Hyper Text Transport Protocol (HTTP). Additional or future methods may be added or approved by the college on a case by case basis.

Electronic Mail – Persons may send e-mail to any account on the network. Prior approval is not required. It is the user's responsibility to maintain the integrity of the college's private e-mail system. Users that have e-mail accounts must keep the account current by deleting or archiving old mail.

Maintenance of the e-mail system will be accomplished by technology support staff through the periodic purging of inactive or non-registered student accounts (dates will be announced). Any subscription to a mail list (or listserv) must be documented with the Computing Services Department at SMC.

Accountability – The only person allowed access to a particular account is the individual in whose name it was issued. Users are responsible for all activity in the account(s) assigned to them. Accounts may not be loaned or shared. Sharing of passwords, accessing someone else's account, or allowing someone else to access your account on SMC's computers (or on an external computer system) is considered a serious violation which will result in loss of privilege. Each user is responsible for all material sent and received under his/her e-mail account.

Audit Trail – SMC will log all user connections while working on the network. The type of connection will be identified and all file transfers while online will be recorded in this log. SMC reserves the right to examine with specific intent any resources associated with user accounts (including remote electronic monitoring of interactive sessions) at any time. All accounts remain the exclusive property of Southwestern Michigan College. If encryption is used in the storing or transmitting of information, a valid key pair must be available to the technology support staff of the Computing Services Department at SMC.

Reporting Violations – Any violations of computer or peripheral device usage, SMC local/wide networks or the Internet must be reported to an instructor, technology support staff, or an administrator. Each user has the responsibility to report any suspected violation of his/her own personal privacy to the administration.

Consequence of Violations – SMC reserves the right to discontinue account privileges to any user who violates the policies of SMC or its network provider. Repeated, or severe, infractions of the policies may result in termination of network privileges permanently. Infractions may result in appropriate disciplinary action in addition to suspension or termination of network privileges. Unauthorized use of the network, copyright violations, or intentional deletion or damage to files and data belonging to the college, other users, or outside agencies may be considered criminal and could result in involvement of governmental authorities. All other acceptable use of computing resources not specifically defined herein is governed by the SMC Board of Trustees.

Inappropriate Use

1. *Users may not access, transfer, or possess pornographic material, inappropriate text files or files dangerous to the integrity of the network, or criminal in nature.*

2. *Users will not engage in anonymous communications or misrepresent themselves to others on the network.*

3. *Malicious use of the network to develop programs or methods that harass other users, including hate-related or discriminatory conduct, or infiltrate a computer or computing system and/or damage or remove the software components of a computer or computing system is prohibited.*

4. *Use of computers, peripherals, or the network to intentionally disrupt the usage, capacity, or performance or otherwise limit computing resources is prohibited.*

5. *Use of the network to intercept, read, translate, or modify transmissions from other network sources is prohibited.*

6. *Installation or execution of copyrighted software, freeware, or shareware that has not been legally acquired by SMC and provided by authorized technology support staff is prohibited. This includes peer-to-peer, demonstration or evaluation software and programs or games representing intellectual property.*

7. *Proliferation of unsolicited e-mail is prohibited. This includes chain letters and all forms of spam.*

8. *Any use of the network for commercial or for-profit purposes is prohibited.*