Policy 5.22
Acceptable Use of Computers and Information Technology Resources

Revised 2/2009

Mesabi Range Community and Technical College has adopted Minnesota State Colleges and Universities' Acceptable Use of Computers and Information Technology Resources, as stated in the MnSCU Board of Directors Policy and System Procedures (Board Policies Chapter 5 – Administration, 5.22 & 5.22.1).

Policy: http://www.mnscu.edu/board/policy/522.html
Procedure: http://www.mnscu.edu/board/procedure/522p1.html

5.22 Acceptable Use of Computers and Information Technology Resources

Policy Statement. Computer and information technology resources are essential tools in accomplishing the mission of Minnesota State Colleges and Universities and its individual institutions. These resources must be used and managed responsibly in order to ensure their availability for the competing demands of teaching, scholarship, administration and other mission-related uses. This policy establishes responsibilities for acceptable use of Minnesota State Colleges and Universities information technology resources.

Part 1. Purpose

Subpart A. Acceptable use. System information technology resources are provided for use by currently enrolled System students, administrators, faculty, other employees, and other authorized users. System information technology resources are the property of Minnesota State Colleges and Universities, and are provided for the direct and indirect support of the System's educational, research, service, student and campus life activities, administrative and business purposes, within the limitation of available System technology, financial and human resources. The use of Minnesota State Colleges and Universities information technology is a privilege conditioned on adherence to this policy and any procedures or guidelines adopted pursuant to this policy.

Subpart B. Academic freedom. Nothing in this policy shall be interpreted to expand, diminish or alter academic freedom, articulated under Board policy and System collective bargaining agreements, or the terms of any charter establishing a System library as a community or public library.

Part 2. Applicability. This policy applies to all users of System information technology, whether or not the user is affiliated with Minnesota State Colleges and Universities, and to all uses of those resources, wherever located.

Minnesota State Colleges and Universities is not responsible for any personal or unauthorized use of its resources. Security of data transmitted on its information technology resources cannot be fully guaranteed.

Part 3. Definitions.

Subpart A. System. For purposes of this policy, System means the Board of Trustees, the Office of the Chancellor, the state colleges and universities, and any part or combination thereof.

Subpart B. System information technology. System information technology means all System facilities, technologies, and information resources used for information processing, transfer, storage and communications. This includes, but is not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, and computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voicemail, facsimile transmissions, video, and multimedia.

Subpart C. Transmit. Transmit means to send, store, collect, transfer or otherwise alter or affect information technology resources or data contained therein.

Subpart D. User. User means any individual, including, but not limited to, students, administrators, faculty, other employees, volunteers, and other authorized individuals using System information technology in any manner, whether or not the user is affiliated with Minnesota State Colleges and Universities.

Part 4. Scope.

Subpart A. Procedures. The chancellor shall adopt procedures under this policy, including, but not limited to: security; employee use, consistent with Minnesota Statutes section 43A.38 and other applicable law; monitoring; unauthorized uses and other limitations on use; and adoption of college and university procedures.

Subpart B. Sanctions. Users who violate this policy or related System, college or university procedures shall be subject to disciplinary action through appropriate channels. Violations may be referred to appropriate law enforcement authorities.

Procedure 5.22.1, Acceptable Use of Computers and Information Technology Resources

for Board Policy 5.22

Part 1. Purpose

Subpart A. Acceptable use. This procedure establishes responsibilities for acceptable use of Minnesota State Colleges and Universities information technology resources. System information technology resources are provided for use by currently enrolled System students, administrators, faculty, other employees, and other authorized users. System information technology resources are the property of Minnesota State Colleges and Universities, and are provided for the direct and indirect support of the System's educational, research, service, student and campus life activities, administrative and business purposes, within the limitations of available System technology, financial and human resources. The use of Minnesota State Colleges and Universities information technology is a privilege conditioned on compliance with Policy 5.22, this procedure and any procedures or guidelines adopted pursuant to this procedure. The System encourages the use of information technology as an effective and efficient tool within the framework of applicable State and federal laws, policies and rules and other necessary restrictions.

Subpart B. Academic freedom. Nothing in this procedure shall be interpreted to expand, diminish or alter academic freedom, articulated under Board policy and System collective bargaining agreements, or the terms of any charter establishing a System library as a community or public library.

Part 2. Applicability

This procedure applies to all users of System information technology, whether or not the user is affiliated with Minnesota State Colleges and Universities, and to all uses of those resources, wherever located. This

procedure establishes minimum requirements and Colleges and universities may adopt additional conditions of use, consistent with this procedure and Policy 5.22, for information technology resources under their control. Minnesota State Colleges and Universities is not responsible for any personal or unauthorized use of its resources, and security of data transmitted on its information technology resources cannot be guaranteed.

Part 3. Definitions

Subpart A. College or university. College or university, except where specified otherwise, means a System college or university, the Office of the Chancellor, or the Minnesota State Colleges and Universities System.

Subpart B. Security measures. Security measures means processes, software, and hardware used by system and network administrators to protect the confidentiality, integrity, and availability of the computer resources and data owned by the System or its authorized users. Security measures may include, but are not limited to, monitoring or reviewing individual user accounts for suspected policy violations and investigating security-related issues.

Subpart C. System. For purposes of this procedure, System means the Board of Trustees, the Office of the Chancellor, each colleges and university within the System, and any part or combination thereof.

Subpart D. System information technology. System information technology means all System facilities, technologies, and information resources used for information processing, transfer, storage and communications. This includes, but is not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, and computing and electronic communications devices and services, such as modems, e-mail, networks, telephones (including cellular), voicemail, facsimile transmissions, video, mobile devices, and multimedia materials.

Subpart E. Transmit. Transmit means to send, store, collect, transfer or otherwise alter or affect information technology resources or data contained therein.

Subpart F. User. User means any individual, including, but not limited to, students, administrators, faculty, other employees, volunteers, and other authorized individuals using System information technology in any manner, whether or not the user is affiliated with Minnesota State Colleges and Universities.

Part 4. Responsibilities of All Users.

Subpart A. Compliance with applicable law and policy.

1. Users must comply with laws and regulations, Board policies and System procedures, contracts, and licenses applicable to their particular uses. This includes, but is not limited to, the laws of libel, data privacy, copyright, trademark, gambling, obscenity, and child pornography; the federal Electronic Communications Privacy Act and the Computer Fraud and Abuse Act, which prohibit "hacking" and similar activities; state computer crime statutes; student conduct codes; applicable software licenses; and Board policies 1.B.1, prohibiting discrimination and harassment; 1.C.2, prohibiting fraudulent or other dishonest acts; and 3.26, concerning intellectual property.
2. Users are responsible for the content of their personal use of System information technology, and may be subject to liability resulting from that use.

3. Users must use only system information technology they are authorized to use and use them only in the manner and to the extent authorized. Ability to access information technology resources does not, by itself, imply authorization to do so.
4. Users are responsible for use of System information technology under their authorization.

Subpart B. Unauthorized use. Users must abide by the security restrictions on all systems and information to which access is authorized.

1. Users must not:

    a. use any account or password assigned by the college or university to anyone else;
    b. share any account or password, assigned to the user by the college or university, with any other individual, including family members;
    c. allow others to use System information technology under the user's control;
    d. use System cellular telephones or computer dial-up services for personal use unless specifically authorized by System or State policy or procedure.

2. Users must not circumvent, attempt to circumvent, or assist another in circumventing security controls in place to protect the privacy and integrity of data stored on System information technology.
3. Users must not change, conceal, or forge the identification of the person using System information technology, including, but not limited to, use of e-mail.
4. Users must not knowingly download or install software onto System information technology unless it has been preapproved through established campus or system office procedures, or by the designated officials, or prior authorization is received from the designated officials. Users who knowingly or negligently do not comply may be held responsible for damages, cost of system debugging, and payment of software fees, licenses and infringement penalties.
5. Users must not engage in activities that interfere with or disrupt network users, equipment or service; intentionally distribute viruses, worms, trojans, or other malicious code; or install software or hardware that permits unauthorized access to System information technology.
6. Users must not engage in inappropriate uses, including:
    a. activities that violate State or federal law or regulation;
    b. wagering or betting;
    c. harassment, threats to or defamation of others, stalking, and/or illegal discrimination;
    d. fund-raising, private business, or commercial activity, unless it is related to the mission of the System or its colleges and universities. Mission related activities are determined by the college, university, or Office of the Chancellor, and include activities of authorized campus or System-sponsored organizations;
    e. storage, display, transmission, or intentional or solicited receipt of material that is or may be reasonably regarded as obscene, sexually explicit, or pornographic, including any depiction, photograph, audio recording, or written word, except as such access relates to the academic pursuits of a System student or professional activities of a System employee; and
    f. "spamming" through widespread dissemination of unsolicited and unauthorized e-mail messages.

Subpart C. Protecting privacy. Users must not violate the privacy of other users and their accounts, regardless of whether those accounts are securely protected. Technical ability to access others' accounts does not, by itself, imply authorization to do so.

Subpart D. Limitations on use. Users must avoid excessive use of System information technology, including but not limited to network capacity. Excessive use means use that is disproportionate to that of

other users, or is unrelated to academic or employment-related needs, or that interfere with other authorized uses. Colleges and universities may require users to limit or refrain from certain uses in accordance with this provision. The reasonableness of any specific use shall be determined by the college or university or Office of the Chancellor in the context of relevant circumstances.

Subpart E. Unauthorized trademark use. Users must not state or imply that they speak on behalf of the System or a college or university, and must not use System, college or university trademarks or logos without prior authorization. Affiliation with the System does not, by itself, imply authorization to speak on behalf of the System.

Part 5. System Employee Users.

All employees of Minnesota State Colleges and Universities are subject to Minnesota Statutes section 43A.38, the code of ethics for employees in the executive branch. In addition to compliance with that statute and this procedure, it is expected that employees will use the traditional communication rules of reasonableness, respect, courtesy, and common sense when using System information technology.

Subpart A. Personal use. In accordance with Minnesota Statutes section 43A.38, subdivision 4, System employees may make reasonable use of System information technology for personal communications as long as the use is in accordance with state law, Board policy and System procedure, and the use, including the value of employee time spent, does not result in an incremental cost to the State, or results in an incremental cost that is so small as to make accounting for it unreasonable or administratively impracticable, as determined by the Office of the Chancellor, college or university. Reasonable use means use consistent with this procedure.

Subpart B. Union activities. In the interest of maintaining effective labor-management relationships and efficient use of State time and resources, System e-mail systems may be used by employee representatives of the union for certain union activities, in accordance with State policy and/or the provisions of applicable collective bargaining agreements.

System-owned property or service, including the e-mail system, may not be used for political activities, fund-raising, campaigning for union office, union organizing activities, or solicitation of employees for union membership.

Union use of electronic communication technology is subject to the same conditions as employee use of such technology, as set forth in Policy 5.22 and this procedure, including security and privacy provisions.

Subpart C. Political activities. System employees shall not use System information technology for political activities prohibited by Minnesota Statutes sections 43A.32 or 211B.09, or other applicable State or federal law.

Subpart D. Religious activities. System employees shall not use System information technology in a manner that creates the impression that the System supports any religious group or religion generally in violation of the Establishment Clause of the First Amendment of the United States Constitution or Article 1, Section 16 of the Minnesota State Constitution.

Part 6. Security and Privacy.

Subpart A. Security. Users shall employ appropriate security practices, including the appropriate use of secure facsimiles or encryption or encoding devices, when electronically transmitting data that is not public.

Subpart B. Privacy. Data transmitted via System information technology are not guaranteed to be private. Deletion of a message or file may not fully eliminate the data from the system.

Subpart C. Right to employ security measures. The System reserves the right to employ security measures, including but not limited to the right to monitor any use of System information technology, including those used for personal purposes. Users have no expectation of privacy for any use of System technology resources, except as provided under federal wire tap regulations (21 U.S.C. sections 2701-2711).

The System does not routinely monitor individual usage of its information technology resources. Normal operation and maintenance of System information technology require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other activities that are necessary for such services. When violations are suspected, appropriate steps shall be taken to investigate and take corrective action or other actions as warranted. System officials may access data on System information technology, without notice, for other business purposes including, but not limited to, retrieving business-related information, re-routing or disposing of undeliverable mail; or responding to requests for information permitted by law.

Part 7. Application of Government Records Laws.

Subpart A. Data practices laws. Government data maintained on System information technology is subject to data practices laws, including the Minnesota Government Data Practices Act and the federal Family Educational Rights and Privacy Act, to the same extent as they would be if kept in any other medium. Users are responsible for handling government data to which they have access or control in accordance with applicable data practices laws.

Subpart B. Record retention schedules. Official college or university records created or maintained electronically are subject to the requirements of the Official Records Act, Minnesota Statutes section 138.17 to the same extent as official records in any other media. Official records must be retained in accordance with the applicable approved records retention schedule appropriate for the type, nature, and content of the record. Willful improper disposal of official records may subject an employee to disciplinary action.

Part 8. College and University Policies and Procedures.

Colleges and universities and the Office of the Chancellor, must adopt policies and procedures consistent with Policy 5.22 and this procedure:

a. for reporting possible illegal activities to appropriate authorities;
b. to implement state and System security policies, procedures, standards and guidelines to protect the integrity of System information technology and its users' accounts;
c. to ensure that government data in electronic format is handled in accordance with its classification under the Minnesota Government Data Practices Act, Family Education Rights and Privacy Act, and other applicable law or policies;
d. to specify the name and contact information of the official to be contacted by users and others if they have questions, concerns or problems regarding the use of System information technology or concerning intended or unintended interruptions of service;
e. for reviewing requests to use the trademarks or logos of the college, university or Minnesota State Colleges and Universities; and

f. to provide information and education to users concerning applicable information technology policies and procedures;
g. for identifying the official(s) designated to make decisions regarding approved hardware or software use.

Part 9. Enforcement.
Conduct which involves the use of information resources to violate a System policy or procedure, or state or federal law, or to violate another's rights, is a serious abuse subject to limitation or termination of user privileges and appropriate disciplinary action, legal action, or both.

Subpart A. Access Limitations. Minnesota State Colleges and Universities reserves the right to temporarily restrict or prohibit use of its System information technology by any user without notice, if it is determined necessary for business purposes.

Subpart B. Repeat violations of copyright laws. Minnesota State Colleges and Universities may permanently deny use of System information technology by any individual determined to be a repeat violator of copyright laws governing Internet use.

Subpart C. Disciplinary proceedings. Alleged violations shall be addressed through applicable System procedures, including but not limited to System Procedure 1.B.1.1 to address allegations of illegal discrimination and harassment; student conduct code for other allegations against students; or the applicable collective bargaining agreement or personnel plan for other allegations involving employees. Continued use of System information technology is a privilege subject to limitation, modification, or termination.

Subpart D. Sanctions. Willful or intentional violations of this policy are considered to be misconduct under applicable student and employee conduct standards. Users who violate this policy may be denied access to System information technology and may be subject to other penalties and disciplinary action, both within and outside of the System. Discipline for violations of this policy may include any action up to and including termination or expulsion.

Subpart E. Referral to Law Enforcement. Under appropriate circumstances, Minnesota State Colleges and Universities may refer suspected violations of law to appropriate law enforcement authorities, and provide access to investigative or other data as permitted by law.

Approved: January 23, 2004

Part 8 of the MnSCU System Procedure requires that Mesabi Range Community and Technical College adopts the following methods for the local implementation of the Board Policy and Procedure:

Part 8. College and University Policies and Procedures.
Colleges and universities and the Office of the Chancellor, must adopt policies and procedures consistent with Policy 5.22 and this procedure:

a. Report possible illegal activities to the Dean of Students, Provost or the Director of Technology

b. Mesabi Range Community and Technical College will implement state and System security policies, procedures, standards and guidelines which will protect the integrity of System information technology and its users' accounts.

c. Mesabi Range Community and Technical College will ensure that government data in electronic format is handled in accordance with its classification under the Minnesota Government Data Practices Act, Family Education Rights and Privacy Act, and other applicable law or policies.

d. If users and others have questions, concerns or problems regarding the use of System Information Technology or concerning intended or unintended interruptions of service please contact:

Director of Technology
Virginia Campus - Room L164
Phone: 218-748-2416

e. Any requests to use the trademarks or logos of the college, university or Minnesota State Colleges and Universities should be directed to the Public Information Officers:
Brenda Kochevar
Public Information Director
Virginia Campus - Room S135
Phone: 218-749-0314
Email: b.kochevar@mr.mnscu.edu

f. The Acceptable Use of Computers and Information Technology Resources policy and procedures and other applicable information technology policies and procedures can be found by the following means:

1. Links to the policy and procedure on the active desktop on all student computers on both campuses.
2. Links to the policy and procedure on the campus website.
3. References to the links to the policy and procedure in the student handbook and the employee guide book.
4. Copies of the policy and procedure will be located in the open labs on both campuses.
5. Reference to the links to the policy and procedure will be in orientation materials for students and new employees.
6. All users will electronically sign the policy and a procedure before their account is activated.

g. The Director of Technology, with the help of the Technology Committee, will make decisions regarding approved hardware or software use.

h. Attaching devices (physically wired, wireless or by any other means) to the campus network is not permitted unless the user has the express permission from the Director of Technology and has filled out the appropriate forms.

i. Any device connected to the campus network must have updated anti-virus software.

j. "Downloading or distributing copyrighted material, including through peer-to-peer file sharing, without the permission of the copyright owner is against the law. Illegal downloading or distribution of copyrighted materials can result in you being prosecuted in criminal court and/or sued for damages in civil court. Criminal penalties for first-time offenders can be as high as five years in prison and $250,000 in fines. If sued in civil court, you may be responsible for monetary damages, attorneys' fees and civil penalties up to $150,000 per work distributed. Use of **Mesabi Range Community and Technical College** resources for unauthorized distribution of copyrighted materials is forbidden."

Review/Revision History:
Implemented at MnSCU 7/16/03
Adopted from MnSCU Policy 5.22 and MnSCU Procedure 5.22.1
Reviewed and Approved through Shared Governance 12/20/05
Revised 2/10/09