Procedure 5.22.1, Acceptable Use of Computers and Information Technology Resources

System Procedures
Chapter 5 - Administration

Click here for a PDF copy of this procedure.
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 system 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, System Procedure 5.22.2 Cellular and Mobile Computing Devices, 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.

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

The definitions in System Procedure 5.22.2, Cellular and Other Mobile Computing Devices, apply to this procedure.

Subpart A. 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 B. System

System means the Board of Trustees, the system office, the state colleges and universities, and any part or combination thereof.

Subpart C. 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, voicemail, facsimile transmissions, video, mobile computing devices, and multimedia materials.

Subpart D. Transmit

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

Subpart E. 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

"hacking" and similar activities; state computer crime statutes; applicable conduct codes, including the System Procedure 1C.0.1, Employee Code of Conduct; applicable software licenses; and Board Policies 1B.1, prohibiting discrimination and harassment, 1C.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 allow others who are not authorized to:

   a. use any account or password assigned by the system to anyone else;
   b. share any account or password, assigned to the user by the system, with any other individual, including family members;

   c. allow others to use system information technology under the user control.

3. 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.
4. 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.
5. Users must not knowingly download or install software onto system information technology unless allowed under applicable procedures or prior authorization has been received.
6. 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.
7. Users must not engage in inappropriate uses, including:

university, or system office, 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, video 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 system office in the context of relevant circumstances.

Subpart E. Unauthorized representations or trademark use

Users must not use system information technology to state or imply that they speak on behalf of the system or use system 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, §43A.38, the code of ethics for employees in the executive branch and System Procedure 1C.0.1, Employee Code of Conduct. In addition, employees are expected to use the traditional communication rules of reasonableness, respect, courtesy, and common sense when using system information technology.

with state law, Board policy and system procedure, including system procedure 5.22.2, 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 system.

Subpart B. Union activities

In the interest of maintaining effective labor-management relationships and efficient use of state time and resources, system e-mail accounts 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 services, 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 system electronic communication technology, as authorized, 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, §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 reasonable physical and technological security measures to protect system records in all phases of handling. This may include, but is not limited to, the appropriate use of secure facsimiles or encryption or encoding devices when electronically transmitting data that is not public.

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 in part 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 requires 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

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.

Part 8. College and University Policies and Procedures

Colleges and universities must adopt policies, procedures and guidelines consistent with Board Policy 5.22 and this procedure:

a. for breach notification or reporting possible illegal activities to appropriate authorities;

d. to specify the name and contact information of the official to be contacted by users and others to address 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;

f. to provide information and education to users concerning applicable information technology policies, procedures and guidelines;

g. for identifying the official(s) designated to make decisions regarding approved hardware or software use.

Part 9. Enforcement

Conduct that involves the use of system information technology 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 or other laws governing Internet use.

Subpart C. Disciplinary proceedings

Alleged violations shall be addressed through applicable system procedures, including but not limited to System Procedure 1B.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 procedure are considered to be misconduct under applicable

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.

Related Documents:

- **Policy 1B.1** Nondiscrimination in Employment and Education Opportunity
- **Procedure 1B.1.1** Report/Complaint of Discrimination/Harassment Investigation and Resolution
- **Procedure 1C.0.1** Employee Code of Conduct
- **Policy 1C.2** Fraudulent or Other Dishonest Acts
- **Policy 3.26** Intellectual Property
- **Policy 5.22** Acceptable Use of Computers and Information Technology Resources
- **Procedure 5.22.2** Cellular and Other Mobile Computing Devices
- **Policy 5.23** Security and Privacy of Information Resources

To view any of the following related statutes, go to the **Revisor's Office website**. You can conduct a search from this site by typing in the statute number.

- Minnesota Statute §136F.46, Non-profit Foundation Payroll Deductions
- Minnesota Statute §136F.80, Grants, Gifts, Bequests, Devises, and Endowments
- Minnesota Statute §136F.81, Transfer of Gifts
- Minnesota Statute §43A.38, subdivision 4, Use of state property

Procedure History:

Date of Adoption: 1/23/04
Date of Implementation: 1/23/04
Date of Last Review:

Date & Subject of Amendments:

grammatical context of the sentence.

Additional **HISTORY**

-