Information Technology Services

Getting Started
Services
Secure Computing
About ITS
- Staff
- IT Strategic Plan
- Projects
- **Policy and Standards**
- Student Technology Fee Committee
- Reports
- Newsletters

Office 365
ITS Home

Policy and Standards

In addition to State of Minnesota and Minnesota State Colleges and Universities policies, St. Cloud State University has these technology-related policies, guidelines and standards in place to help users understand how technology should be used at our university for the benefit of the campus community as a whole.

The guidelines address accountability, provide consistency and establish procedures for those who use the university's equipment and network.

University and IT Policies

- University Data Practices Policy
- University Email Policy
- Technology Account Access and Management
- ResNet and Open Data Jack Acceptable Use Policy
- Community Patron access policy
- Web Standards Policy

+ Minnesota Policies and Laws

+ Reporting Technology Abuse

Guidelines and Standards

− E-mail Acceptable Use Guidelines

Purpose

St. Cloud State University (St. Cloud State) provides many computing and network resources for use by students, faculty, staff and other persons affiliated with St. Cloud State. Members of the university community are encouraged to use electronic mail (e-mail) for university-related activities to facilitate the efficient exchange of useful information. Access to e-mail is a privilege and certain responsibilities accompany that privilege. Users of e-mail are required to be ethical and responsible in their use.

Electronic mail is one of the most used and useful facilities on computer networks. To ensure maximum benefits from e-mail, a clear, defined balance between the need for open communication and the protection of the university's assets is critical.

The purpose of this policy is to encourage use of e-mail as an effective and efficient tool within the framework of the appropriate Minnesota and federal laws, University policies and rules and other necessary restrictions apply even if they are not specifically mentioned in this policy. For example, employees should bear in mind the responsibility of the Statewide Electronic Communication and Technology Ethics Policy, and the terms of any other applicable standard of conduct.

Privacy

Although the University does not routinely monitor all messages, it does have the authority, at any time, to inspect the contents of any University equipment, files, or mail on its system for any legitimate business, legal or disciplinary purpose. Reasons for review include, but are not limited to: reasonable suspicion of a violation of a rule or law or University policy; investigation of system problems; litigation or anticipated litigation; a need to perform work when an employee is not available.

Employee users of the University's e-mail system must understand that most communications created, received or backed up on the system are considered to be public documents and thus, may be subject to requests for public disclosure. Employees should bear in mind that this construction may apply even to e-mails that contain, for example, personal remarks.

Users must respect the integrity and security of the system. A user's account and password are the keys to the e-mail network, and users are advised that they are responsible for the security of their respective account and password. There are major risks when a user's account and password are known to others.

By law certain data is not available to the public, such as personal or non-directory education data ("not public data"). If e-mail is used to transmit such data, it should be clearly labeled as not public. Designating messages in this manner may reduce the possibility that the recipient will disclose the data to unintended third parties, but users must take appropriate care to protect not public data and disclose it only to persons who are legally entitled to access. Users who illegally disclose not public data will be subject to discipline.

Principles of Acceptable Use

Access to and the responsible use of modern information resources are essential to the pursuit and achievement of excellence at St. Cloud State. The University encourages appropriate use of e-mail to enhance productivity through the efficient exchange of information in education, research, public service and the expression of ideas. Use of these resources must be consistent with these goals. As responsible members of the St. Cloud State community, everyone is expected to act in accord with the following general principles based on the acceptable law as well as common sense, common decency, and civility applied to the networked computing environment:

Messages sent as electronic mail should meet the same standards for distribution or display as if they were tangible documents or instruments. Identify yourself clearly and accurately in all electronic communications. Concealing or misrepresenting your name or affiliation to dissociate yourself from responsibility for your actions is never appropriate. Alteration of the course of electronic mail, message or posting is unethical and may be grounds for discipline. One test of appropriateness would be to never “say” anything via e-mail that you would not be willing to say directly to a person.

Be sensitive to the inherent limitation of shared network resources. No computer security system can absolutely prevent a determined person from accessing stored information, and St. Cloud State cannot guarantee the privacy or confidentiality of electronic documents.

Respect the rights of others. Do not send abusive, threatening, or harassing materials. Civil discourse is at the heart of a university community free of intimidation and harassment and based upon a respect for individuals as well as a desire to learn from others. While debate on controversial issues is inevitable and essential, you may not use the University's electronic communication in a manner that violates the University's policies or applicable laws against discrimination or harassment including policy and laws against sexual harassment. The same standards or conduct expected of students, faculty and staff regarding the use of telephones, libraries, and other institutional resources apply to the use of e-mail. You will be held no less accountable for your actions in situations involving e-mail than you would be in dealing with other media.

It is unacceptable to use the University's system to engage in wasteful and disruptive practices, such as creating or sending “chain letters”, “broadcast” messages or unwanted material, “flaming”, or overloading a system. This effort is consistent with existing practices governing other forms of communication on campus including telephone calls, bulletin board postings, the mass distribution of fliers and the use of intra-campus mail services.

In accordance with the Minnesota Department of Employee Relations Administrative Procedure No. 32, and Minnesota Statute Section 43A.38, Subd. 4, political transmissions are prohibited. This would include transmissions which advocate the election of particular candidates for public office at either the federal, state or local level. This also prohibits sending of messages which contain information on religious positions or activities. Also banned are those messages that advocate support of or opposition to any particular referendum proposal that will be decided by the voters during the general or special election affecting the public at large.Those using e-mail for legitimate educational purposes should be careful to abide by the statute cited above; other examples of inappropriate personal use of the system include, but are not limited to, wagering, fundraising for any purpose unless University-sanctioned or promotion of religious positions or activities.

E-mail and other network resources may not be used for commercial purposes or for personal financial gain. To do so would be a violation of Minnesota state law. This does not preclude the use of e-mail to assist in the investigation and support of vendor's products, such as the discussion of a product's relative advantages and disadvantages by users of the product, the distribution of information or technical support material by request or vendor responses to questions about their products, as long as the responses are not in the nature of a solicitation.

You are expected to abide by the security restrictions on all systems and information to which you have access. Activities that interfere with or disrupt network users, equipment or services including the intentional distribution of viruses or seeking unauthorized access to machines on the network are prohibited.

Conduct which involves the use of information resources to violate a university policy or regulation or state or federal law, or to violate another's rights, is a serious abuse subject to limitation of your privileges and appropriate disciplinary and/or legal action. The University is not responsible for transmissions which are libelous or defamatory, but will appropriately investigate and address these unwanted transmissions with the message sender. If unsolicited or unwanted Internet transmissions are received, or if problems or issues arise regarding St. Cloud State e-mail, you should contact Husky Tech.

E-mail managers and network system administrators should not monitor or access the contents of electronic files except as noted in this policy.

Complaints

Complaints by any user receiving electronic transmissions through any e-mail server may be submitted to the:

- Chief Information Security Officer (Eric Hanson)
- Deputy Chief Information Officer (Phil Thorson)

The Affirmative Action Office will be notified of complaints regarding the transmission of discriminatory material. One of the Information Services Directors will work with Campus Security and/or other appropriate offices to investigate the complaint to make a determination of its validity. In the case of an employee investigation, if a violation did occur, the Campus Security Director shall inform the employee's immediate supervisor and other appropriate offices. The employee's immediate supervisor, in consultation with other University offices, shall impose proper action in a form and process consistent with public employee laws and collective bargaining agreements.

These guidelines are subject to change.

+ SCSU-Announce and SCSU-Discuss Listserv Guidelines

+ Technology Downtime Schedule

Information Technology Services
Contact Information
Phone: (320) 308-7000

Campus address
720 4th Avenue South
St. Cloud, MN 56301-4498
(320) 308-0121