# Responsible Use of Computing Resources Policy

**Policy number:** 108
**Policy owner:** Chief Information Officer

## Overview

The University of St. Thomas encourages computer use in accordance with its mission and purpose by providing computing resources to the university community. This Policy describes the University's guidelines and policies governing responsible use of computing resources by students and employees.

## I. Acceptable Uses of University of St. Thomas Computing Resources

Computing resources are intended for instruction, study, academic research, and the official work of campus organizations and university offices. In addition, as with any resource on campus, access to academic computing resources is provided, in part, to allow members of the community to learn, explore, and grow.

*All users of University computing resources must:*

1. Comply with all federal, Minnesota and other applicable law, with all applicable University rules and policies, and all applicable contracts and licenses.

2. Use only those computing resources that they are authorized to use, and use them only in the manner and to the extent authorized.

3. Respect the privacy of other users and their accounts.

4. Respect the limited capacity of the University's computer resources, and limit use so as not to consume an unreasonable amount of those resources or to interfere unreasonably with the activity of other users.

5. Protect their usernames and passwords from unauthorized use.

6. Access only information that is one's own, or that is publicly available, or to which one has been given authorized access.

7. Cooperate with system administrators if advised of potential security problems associated with their accounts or systems.

## II. Unacceptable Uses of University of St. Thomas Computing Resources

*Conduct which constitutes unacceptable use under this Policy includes, but is not limited to:*

1. Accessing another person's computer, files or data without permission. This includes data in transit on the network.

2. Using a system or the network to obtain unauthorized access to or deny services to any offsite system. Such actions may also violate federal law.

3. Circumventing, violating, or subverting system or network security measures, or exploiting flaws in same, or attempting to do so. Examples include: circumventing the computer registration processes and procedures for address assignment; creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system. If you find a hole in the security of any St. Thomas system, notify Information Technology Services (ITS) staff immediately at (651) 962-6230.

4. Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, such as creating or propagating viruses, disabling or habitually circumventing virus protection, disrupting services or damaging files or making unauthorized modifications to University data. For example, using Outlook to bring email into a St. Thomas Exchange mailbox directly from a different mail system that has not implemented responsible virus and spam controls and thereby introducing a steady stream of infected messages to the St. Thomas system from within.

5. Performing any act that will, intentionally or otherwise, interfere with the normal management or operation of computers, terminals, peripherals or networks, including altering ITS's level of access to a university system.

6. Using University systems or content (including subscribed library electronic databases) for personal gain, for commercial purposes or for partisan political purposes; for example, selling access to a University user id or to University systems or networks; performing work for profit with university resources in a manner not authorized by the University; or using electronic mail to circulate advertising for products.

7. Making or using illegal copies of copyrighted software or data, here defined to include text, audio, video or other files of course materials, presentations, or other communications where not authorized, restoring such copies on University systems, or transmitting them over University networks. Unless given explicit permission by the copyright holder, you may not copy software or computer data, including audio or video data, available through the University. You may not place copyrighted material on any computer connected to the St. Thomas network for the purpose of making it available for others to copy unless you own the copyright or can demonstrate a teaching or research fair-use exemption from copyright. Software piracy, and the swapping of copyrighted music, movies, or other media content, constitute theft and will expose the both the person sharing and the person copying to lawsuits and possibly to criminal charges.

8. Using University software or data, including electronic mail, to harass or intimidate another person.

9. Saturating network or computer resources to the exclusion of another's use, for example, overloading the network with either legitimate (file backup, archiving, bulletin boards, synchronous chat sessions) or malicious (denial of service attack) activities.

10. Sharing your username and password with others. Providing access to St. Thomas systems or networks to users who do not have an official affiliation with the University without ITS permission is prohibited. This includes providing user accounts on personal systems (i.e. Unix shell accounts, PC-Anywhere passwords, or any such analog). If permission is granted, the administrator of that system is responsible for all user activities on that system.

11. Attaching any device other than a personal computer to the campus network without the express permission of Information Technology Services staff. This includes (but is not limited to) wireless access points such as the Apple AirPort, hubs, switches, routers, printers, and protocol analyzers.

12. Abusing email.

    *The following activities specific to email use are prohibited:*

    - Spoofing sender addressing, that is, forging the identity of a user or machine in an electronic communication
    - Failing to comply with a request to stop emailing someone or to take them off a distribution list
    - Sending all-campus email messages
    - Creating or forwarding chain letters
    - Initiating or facilitating in any way mass electronic mailing (e.g., \"spamming\", \"flooding\" or \"bombing\") except for purposes of conducting University business, and then only with the advice and consent of Information Technology Services regarding when and how to send the mail

    Taken together, these rules do not preclude sending non-work-related email to large lists of other users. However, group mailings should be targeted to people who might reasonably be construed to have an interest in the material, and senders must honor all requests to be excluded from similar future mailings.

## III. Applicability of Other University Codes of Conduct

All St. Thomas codes of conduct, including those related to plagiarism, harassment and unauthorized use of course materials, apply also to technology resources. These policies are based on respect for the work and privacy of other St. Thomas community members.

## IV. Data Privacy

Files and email stored on or transmitted across university systems are not guaranteed to be private. Given the possible application of professional duties of confidentiality, confidential email, files, and other data of designated members of the School of Law, the College of Applied Professional Studies, and the School of Social Work will not be examined for content nor disclosed without the prior approval of the Dean of each school. While as a general policy, University employees will not read your email or private files the St. Thomas reserves the right (as permitted by state and federal law) of designated ITS staff to log and examine any and all network traffic on the university data network, and to retrieve and examine any and all files stored on St. Thomas systems, both central servers and desktops, whenever necessary, particularly but not exclusively in the following situations:

- If information is required in a court proceeding. Electronic data, including deleted information that has been restored from back-up tape, has been subpoenaed as evidence during both civil and criminal court cases. If such a situation arises, the university is legally bound to cooperate with law enforcement authorities and to fulfill lawful requests for information.
- If an individual is suspected of an infraction of University policy or of the law (e.g., engaged in unacceptable use of St. Thomas computing resources as outlined in this

Policy), Information Technology Services will act as the investigating office and will involve other campus offices as needed.

- If an individual's private files (electronic or email) are wanted as evidence on a non-computer-related university disciplinary matter (such as an academic dishonesty case or a sexual harassment investigation), ITS will provide those files on request of Dean of Students, the General Counsel or Associate General Counsel, the dean of the appropriate college, or the Associate Vice President of Human Resources.
- Unless the infraction involves potentially criminal behavior, ITS will make an effort to inform the individual that their files are being examined.
- If a state or federal agency (BCA, FBI, etc.) requests the data as part of an authorized investigation

## V. Enforcement

The University considers violations of acceptable use principles to be serious offenses. The University will take such action as is necessary to copy and examine any files or information resident on University systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations.

In the case of minor infractions, ITS will attempt to contact the offending party via email, telephone or in person to explain the problem and discuss its resolution. Blatant violations or repeated offenses will be referred to the appropriate University entity for discipline.

In the case of major infractions, for example those that impair others' ability to use networking and computing resources, ITS may restrict systems or network access as it deems necessary to mitigate such activities. Only thereafter will ITS make a reasonable effort to contact the involved parties when these incidents occur.

Violations of this policy will result in disciplinary action by the Dean of Students, Associate Vice President of Human Resources, and other appropriate authorities, if necessary. ITS staff may take immediate action as needed to ensure system integrity. This may include, but not be limited to, immediate denial of access to your account, loss of email privileges or removal of your system from the network. In cases involving violations of this Policy or other campus codes, the relevant disciplinary offices will be given all information about an incident that ITS can collect. ITS will advise and testify as requested, and if asked to disable accounts as a result of disciplinary hearings, will do so with all possible speed. The University Site Security Policy contains more detailed information about the processes of investigations.

## VI. Further Information

If you have any questions about whether an activity is permissible or not, you may call the ITS Tech Desk at (651) 962-6230 or the Office of the Dean of Students at (651) 962-6050.