

Acceptable Use Guidelines

This document is intended to provide users of the University's computer systems and networks guidelines concerning what constitutes appropriate and inappropriate use of University owned and operated technology resources. This list of guidelines is not intended to be a complete list of all possible technologies or uses.

The official policy governing acceptable use is the Acceptable Use Policy

Institutional Purpose Guidelines

- Use resources for authorized purposes only
- Access only information that is your own, that is publicly available, or to which you have been given authorized access.
- Use only legal versions of copyrighted software in compliance with vendor license requirements.
- Seek authorization from the Network and Campus Computing Department before installing any software of any kind on any University system including computer labs. Such software includes but not limited to personally licensed software, shareware, or freeware programs.
- Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, degrading services, or wasting computer time, connect time, disk space, printer paper, manuals, or sending chain letters or unsolicited mass mailings or other resources. Participation in these activities is not only unethical, but may constitute harassment.
- Do not use university systems for commercial or partisan political purposes. For example, do not use email to circulate advertising for products or for political candidates.
- Do not use mail or messaging services to harass or intimidate another person, for example, by broadcasting unsolicited messages, by repeatedly sending unwanted mail, or by using someone else's name or username.
- Do not distribute pornography or other questionable material.
- Do not attempt to disrupt operation of any system or network.
- Do not install any unlicensed software on any University system.
- Do not make unauthorized/unlicensed copies of any University-owned software.
- Do not make or use illegal copies of copyrighted materials (software, documents, sounds, pictures), store such copies on university systems, or transmit them over university networks.
- Do not publish or share confidential information.
- Do not use departmental or individual computing resources, such as a personal or departmental laser printer or faxes for any use not directly related to the mission of the University.
- Do not display on-screen images, sounds or messages that could create an atmosphere of discomfort or harassment of others.

Security Guidelines

- Protect your username and systems from unauthorized use. You are responsible for all activities by your username or that originate from your system. For example, never leave a computer unattended without first locking the computer or logging out.
- Select a password that is not easily guessed and do not share the password with anyone. A poorly chosen password may result in the compromise of the University of St. Thomas' entire network. For security reasons, it may be necessary on occasion for the University to implement a system-wide change of passwords.
- Be aware of computer viruses and other destructive computer programs and take steps to avoid being a victim or unwitting distributor of these programs. For example, do not open any files or macros attached to an email from an unknown, suspicious or untrustworthy source.



Delete these attachments immediately, then "double delete" them by emptying your Trash.

- Do not use another person's system, files, or data without permission.
- Do not use another person's computer accounts, passwords, and other types of authorization that are assigned to individual users. You are responsible for all activity occurring from your account. Abuse of an account on the University systems is traced back to the owner of this same account.
- Do not use computer programs to decode passwords or access control information.
- Do not attempt to circumvent or subvert system or network security measures.
- Do not engage in any activity that might be purposefully harmful to systems or information stored on these systems, such as creating or propagating viruses, disrupting services, or damaging files or making unauthorized modifications to university data.

To report a violation, send an email to abuse@stthom.edu.

If you have any questions about these guidelines, please refer to the Acceptable Use Policy.