

Network Use Policy

Stonehill College

24 August 2006

Foreword

The Stonehill College Network Use Policy is administered by the Department of Information Technology. The purpose of this policy is to protect both the College and the users of the Stonehill Network. This policy is subject to change.

Table of Contents

[1 Introduction](#)

- 1.1 Mission Statement
- 1.2 Services Available
- 1.3 Who is a Member of the Network Community

[2 Privileges and Rights of Network Community Members](#)

- 2.1 Privacy
- 2.2 Equal Access
- 2.3 Safety
- 2.4 Intellectual Freedom

[3 Responsibilities of Network Community Members](#)

- 3.1 Passwords
- 3.2 Network Degradation
- 3.3 Copyrights
- 3.4 Privacy
- 3.5 Illegal Activities
- 3.6 Computer Viruses
- 3.7 Inappropriate Language
- 3.8 Personal Attacks
- 3.9 Impersonation
- 3.10 Standards of Behavior
- 3.11 Business Transactions
- 3.12 Unauthorized Access
- 3.13 Network Interference
- 3.14 Configuration Control
- 3.15 Property Control
- 3.16 Equipment Modification
- 3.17 Violation reporting
- 3.18 External Investigations
- 3.19 Network Applications
- 3.20 Remote Server Services

[Appendix: Privacy Considerations](#)

Section 1: Introduction

Stonehill College provides all faculty, staff, administrators, and students with free, open, and easy access to the Internet. Network use is governed by this Network Use Policy and is subject to Federal, State, and local laws, and Stonehill College regulations. The college owns 100% of the network leading from a personal computer to the Internet; it requires that all users connected to the network adhere to this acceptable use policy and other applicable regulations. The Stonehill College Network consists of the individual computers and terminals, servers, network routers/switches/hubs, and the physical interconnections. Individuals who violate this policy may lose network access. Members of the Information Technology Department have the authority to temporarily revoke network access until an incident is reviewed by the college administration.

The Electronic Communications Privacy Act of 1986 ("ECPA") was an outgrowth of the Wiretap Act adopted in the late 1960s. It was enacted because of a growing concern with the possibility that electronic communications were vulnerable. Individuals with expertise in communications engineering can easily monitor private communication with total disregard for privacy considerations. Worried that this would amount to widespread abuse of power, Congress enacted the ECPA to protect the privacy of electronic communications. Under the act, anyone who intercepts, or attempts to intercept, electronic communication is subject to prosecution. The ECPA also prohibits the disclosure or use of stored communications. There are several exceptions to these ECPA provisions. If the system or network has public access there is no interception violation. Also, it is not a violation of the ECPA to engage in otherwise prohibited activity that is necessary incident to the rendition of services, or to protection of the property of the provider of the service. It is legal for a provider to allow interception or disclosure/use of communications when presented with justifications from the proper legal authorities. If at least one party to a communication consents, it does not constitute an ECPA violation to intercept a message.

In using the Stonehill College network users are granting permission for authorized network administrators to monitor and/or intercept electronic communications. Since use of the Stonehill College network is consent to intercept and/or monitor communications, Stonehill College network administrators are not subject to intercept violations. Use of the Stonehill network is consent to interception of communications.

Electronic mail (e-mail) transactions traversing the Internet are not secure nor protected by the laws that apply to the Postal Service. The Internet is a public packet network. There is no legislation to prosecute people who intrude into the public segment of the electronic mail system. The e-mail you send from a machine on the Stonehill network is considered College business and is not private property. It can be legally intercepted and read by those charged with monitoring the system. Although wide latitude is permitted in using e-mail, some uses are prohibited. Among these are conducting a private business and sending off-color, sexist, or racist comments.

1.1 Mission Statement

Stonehill College provides network access to the Stonehill Community for Academic endeavors consistent with the mission of the College. This provides community members with the opportunity to have ease of access to information, but also requires community members to accept certain responsibilities. It is the responsibility of the Academic Computing Department to provide the network services; the user shall be responsible for using the services in accordance with all applicable laws and regulations. The Internet is an invaluable resource for research and communication, but it also contains information that is counter to the aims and objectives of Stonehill College.

1.2 Services Available

As the Stonehill College Network grows and evolves, services will be added and terminated. These may include: various ways of accessing the Internet, such as electronic mail (e-mail), Usenet news, the world wide web, gopher, screen sharing, and desktop video teleconferencing; access to file server storage space; information on types of software available, kinds of printing access, types of computers available, who provides computer help and support, etc.

1.3 Who is a Member of the Network Community?

It is important to be aware of the many people, here at Stonehill College and throughout the Internet, that might be a part of your electronic community. Think about the sensibilities of these people when you post messages or send e-mail. Our Stonehill community consists of students, faculty, staff, administrators, and religious.

Section 2: Privileges and Rights of Network Community Members

Members of the network community have certain privileges and rights. Infringement of, or disrespect for, the rights of others may result in the loss of your network privileges. These rights include:

2.1 Privacy

All members of the network community have a limited right to privacy in their personal electronic communications. However, if a user is believed to be in violation of the guidelines stated in this policy, a system administrator may need to gain access to private correspondence or files. System administrators also may need to access private files as part of regular system maintenance. An attempt will be made to notify the user of this in advance whenever possible. It is important that users recognize the fundamental differences between public (e.g., news or aliased e-mail) and semi-private (e.g., e-mail) forms of communication, and shape their content accordingly.

2.2 Equal Access

All members of the network community will generally be granted free and equal access to as many network services as their technology allows, but the College reserves the right to impose appropriate restriction from time to time. Exploration of the Internet is encouraged relative to the

purposes of the College's Network; however, no single user should monopolize a computer or the network it uses. You may be asked to remove personal files if total system storage space becomes inadequate.

2.3 Safety

To the greatest extent possible, members of the network community will be protected from harassment and unwanted, or unsolicited contact. Any community member who receives threatening or unwelcome communications should bring them to the attention of Director of Information Technology. Users must, however, be aware that there are many services available on the Internet that could potentially be offensive to certain groups of users. The designers of this network cannot eliminate access to all such services, nor could they even begin to identify them. Thus individual users must take responsibility for their own actions in navigating the network.

2.4 Intellectual Freedom

The Stonehill College Network must be a free and open forum for expression, including viewpoints that are strange, unorthodox, or unpopular. However, anyone who posts an opinion should be aware that other community members may be openly critical of such opinions. Occasionally, a posted message may be met from outside the local network community with especially harsh criticism (a practice known as "flaming"). It is best not to respond to such attacks, unless you believe you are capable of a measured, rational reply. Personal attacks are not an acceptable use of this network at any time. This organization does not officially endorse any opinions stated on the network. Any statement of personal belief is implicitly understood to be representative of the author's individual point of view, and not that of Stonehill College.

Section 3: Responsibilities of Network Community Members

With the rights and privileges of membership in the network community come certain responsibilities. Users need to familiarize themselves with these responsibilities. Failure to adhere to them may result in the loss of network privileges:

3.1 Passwords

Never share your password or account with anyone. You have full responsibility for the use of your account. All violations of this policy that can be traced to an individual account name will be treated as the sole responsibility of the owner of that account. Under no conditions should you give your password to another user.

3.2 Network Degradation

Do not knowingly degrade the performance of the network. Electronic chain letters^[1] and mail bombs^[2] are prohibited for this reason.

3.3 Copyrights

Network community members must respect all copyrights, including copyrights in software, and always provide proper attributions of authorship. Commercial software licensed to Stonehill College may only be installed on a College system. Commercial software licensed to Stonehill College shall not be installed on personal systems. Users who install commercial software licensed to themselves are responsible for respecting the licensing agreements. Upon request from a network administrator, individuals who have software licensed to themselves installed on Stonehill machines shall produce original disks, and/or documentation to verify compliance.

3.4. Privacy

Posting personal communications to a public forum without the original author's prior consent is prohibited. To do this is a violation of the author's privacy. However, all messages posted in a public forum, such as news groups or aliased e-mail, may be copied in subsequent communications, as long as proper attribution is given (unless the author has expressly or impliedly prohibited such copying - reproduction without consent may violate the author's copyrights).

3.5 Illegal Activities

Use of the network for any illegal activity is prohibited. Illegal activities include tampering with computer hardware or software, unauthorized entry into computers, or knowledgeable vandalism or destruction of computer files. Users must not defeat or attempt to defeat Stonehill College security systems, such as "cracking" or guessing user identifications or passwords, compromising room locks or alarm systems. Such activity is considered a crime under state and federal law.

3.6 Computer Viruses

Avoid the knowing or inadvertent spread of computer viruses. "Computer viruses" are programs that have been developed as pranks and can destroy valuable programs and data. Deliberate attempts to degrade or disrupt the system performance of the Stonehill College Network, or any other computer system or network on the Internet, by spreading computer viruses, is considered criminal activity under state and federal law.

3.7 Inappropriate Language

Profanity or obscenity will not be tolerated on the Stonehill Network, nor will discriminatory or similarly offensive comments that address someone's race, gender, sexual orientation, religious or political beliefs, natural origin or disability. All community members should use language appropriate for Stonehill College.

3.8 Personal Attacks

Avoid offensive or inflammatory speech. Community members must respect the rights of others both in the local community and in the Internet at large. Personal attacks are an unacceptable use

of the network. If you are the victim of a "flame," bring the incident to the attention of a College official or system administrator.

3.9 Impersonation

Impersonation, anonymity, or pseudonyms are not permitted.^[3]

3.10. Standards of Behavior

Exemplary behavior is expected on "virtual" field trips. When "visiting" locations on the Internet or using video conferencing or screen-sharing communication tools, community members must conduct themselves as representatives of the Stonehill College community as a whole. Conduct that is in conflict with the responsibilities outlined in this document will be subject to loss of network privileges.

3.11 Business Transactions

Use of the network to operate a business enterprise is strictly prohibited. Without specific authorization, all activities using Stonehill College's facilities for personal profit or for the direct financial benefit of any non-Stonehill organization are prohibited. However, this is not meant to restrict normal communications and exchange of electronic data, consistent with the College's education and research roles, that may have an incidental financial or other benefit for an external organization. For example, it is appropriate to discuss products or services with companies doing business with Stonehill or to contribute to Usenet bulletin boards discussing issues relating to commercial products. It is also appropriate to conduct occasional private business transactions such as ordering merchandise from a retail presence on the Internet.

3.12 Unauthorized Access

Users must not make or attempt to make any unauthorized access to, or changes in, data on a Stonehill College device, such as reading personal communications of other users or accessing confidential files. Users must not intercept, or attempt to intercept, data communications not intended for their access, such as by promiscuous bus monitoring^[4] or wiretapping.

3.13 Network Interference

Users must not deny or interfere with, or attempt to deny or interfere with, service to other users; e.g., "resource hogging," distribution of computer worms or viruses, etc.

3.14 Configuration Control

Without specific authorization^[5] users of Stonehill computing or network facilities must not cause, permit, or attempt any destruction or modification of data or computing or communications equipment, including but not limited to alteration of data, reconfiguration of control switches or parameters, or changes in firmware. This rule seeks to protect "data,

computing, and communications equipment" owned by Stonehill College, or any other person or entity.

3.15 Property Control

Without specific authorization by the owner or designated administrator, users must not remove any Stonehill-owned or -administered equipment or documents from a Stonehill College facility. Without specific written authorization from the Academic Dean no equipment or software shall be taken to an employee's residence or other off-campus site. The Department of Information Technology shall have the right and responsibility to inspect the hardware and software configuration on Stonehill computers or personal computers connected to the Stonehill Network. Members of the Department of Information Technology shall be authorized to make appropriate changes to any machine connected to the Stonehill Network that they deem are necessary to ensure proper network operation. Reasonable attempts will be made to contact the primary user of the equipment first.

3.16 Equipment Modification

Without specific written authorization^[6], users must not physically or electrically attach any foreign device (such as an external disk, printer, or video system) to Stonehill College equipment.

3.17. Violation Reporting

Users must report any evidence of violation of these rules to the Director of Information Technology or other College authorities. Users must not conceal or help to conceal violations by any party. The policies described herein are those that Stonehill College intends to use in the normal operation of its facilities. This document does not waive any claim that Stonehill College may have to ownership or control of any hardware, software, or data created on, stored on, or transmitted through Stonehill College facilities.

3.18 External Investigations

If you are contacted by a representative from an external organization (District Attorney's Office, FBI, IDT security, NYNEX security, etc.) who is conducting an investigation of an alleged violation involving Stonehill College's computing and networking resources, you must immediately inform the Director of Information Technology. Refer the requesting agency to the Director of Information Technology; the Director of Information Technology will provide guidance regarding the appropriate actions to be taken.

3.19 Network Applications

Users will not delete or interfere with the use of network applications to monitor operating software on Stonehill computers.

3.20 Remote Server Services

Remote access to the Stonehill Network represents a major security risk. No member of the Stonehill community shall install any remote access software on any computer connected to the Stonehill network without approval from the Director of Information Technology and the Academic Dean. No user, without the explicit permission of the Director of Information Technology, shall install any web server, ftp server, or other remote information server software on any computer connected to the Stonehill Network.

Appendix

Privacy Considerations

It is the policy of the Academic Division to ensure the greatest degree of confidentiality in treating user data on Stonehill College systems and networks consistent with available technology and the need for system maintenance, backups, troubleshooting, etc. The situation will vary somewhat depending on what system or network is being used. Users should be aware of the following considerations.

- a. Data storage and communications are not perfectly secure. There are software and physical limitations that can compromise security. The Department of Information Technology tries to minimize such exposures, but the risks exist. Example: A bug in a utility program might allow one user to read another user's files, or a user might tap a data network wire to view data that is flowing to another user's machine.
- b. Data files residing on disk can be periodically backed up to magnetic tape, and some of these backups are kept for long periods of time. All user files may be backed up this way, although some "scratch" or transient files may not. The Department of Academic Computing does not guarantee the availability of backups to restore user files deleted through errors.
- c. Certain utility programs allow users to view other users' activity on a computer system or network.
- d. Users must be aware of the protection level assigned to their files and directories. The user shall be responsible for the proper use of commands to set any other desired protection level.
- e. Certain system activities are routinely logged, and the logs may be readable by other users. The intention of logging is to collect statistics and diagnose system problems. Example: On the mail servers, logs of mail messages sent or received (sometimes including text) are maintained. In rare cases, detailed logs of each command invocation may be kept.
- f. In cases of suspected violations of network use policies, especially unauthorized access to Stonehill College systems, the Director of Information Technology may authorize detailed session logging. This may involve a complete keystroke log of an entire session. In addition, the director of the Academic Division may authorize limited searching of user files to gather evidence on a suspected violation.

g. On certain systems, users may have the option of encrypting data files. While this may offer good security against unwanted access, the proper use of encryption is the responsibility of the user. If the encryption key is lost, the Department of Information Technology cannot recover the data.

h. Privacy depends on users keeping their account password secure. Users must have "good" (difficult to guess or "crack") passwords and must not share their passwords with other persons. The policy of the Department of Information Technology is that a user password should be at least six characters and not be a dictionary word. Passwords should not be names of family members, dates of birth, vehicle registration numbers, etc...

This list indicates a number of limitations of user privacy and confidentiality. Notwithstanding these limitations, the Department of Information Technology will make all reasonable efforts to maintain confidentiality of user data. Information Technology staff are forbidden to "browse" user files without specific purpose and authorization. If, by mistake or other cause, an Information Technology staff member reads protected user information, he or she will not divulge this information except as authorized by the Director of Information Technology or by appropriate legal authorities.

[1] E-mail messages equivalent to traditional chain letters promising luck or money if the receiver forwards the message to a number of other individuals.

[2] To send, or urge others to send, massive amounts of email to a single system or person, especially with intent to crash the recipient's system. Sometimes done in retaliation for a perceived serious offense. Mail bombing is itself widely regarded as a serious offense because it can disrupt email traffic or other facilities for innocent users on the victim's system, and in extreme cases, even at upstream sites.

[3] As an educational network, we believe that individuals must take responsibility for their actions and words.

[4] The practice of programming a network interface to intercept all network traffic, not just the traffic addressed to that particular network interface.

[5] Specific authorization refers to permission by the owner of the equipment or data to be destroyed or modified, or by a Department of Information Technology System Administrator.

[6] The written authorization shall be issued by the Department of Information Technology and validated by the office of the Academic Dean.