Computing and Information Resources and Privileges

Access to computing facilities and associated resources is provided as a privilege to members of the Silver Lake College community. The college provides these resources to support its educational mission. It is expected that users will obey all rules and regulations pertaining to the appropriate use of these facilities. This involves using the facilities in a manner that is consistent with all-college policies, with policies of other networks (e.g., WISCNET, Internet), and with state and federal laws. Every user is responsible for helping to ensure that these resources are used appropriately; this includes prompt reporting of instances where it is believed an abuse has occurred. If users are in doubt as to whether a particular proposed use is appropriate, they should check with Information Technology staff before the proposed use is undertaken. Misuse of computing facilities (whether or not they are directly college-owned) will constitute just cause for disciplinary action by Silver Lake College in addition to any legal enforcement by local, state, or federal authorities.

The following are guidelines for the appropriate use of computing facilities:

1. Use Facilities and Services Only for the Purposes for Which You Are Authorized. Violations include:

a. using another person's account or attempting to capture/guess other users' passwords;

b. circumventing normal resource limits, log-on procedures, and security regulations;

c. trying to obscure your true identity as the sender of electronic mail or the user of other networked services that request identification;

d. using college computing resources for unauthorized commercial purposes; and

e. using the college's computing resources to harass, intimidate, or threaten other users.

2. Respect the Privacy of Other Users

Files, tapes, disks, email, information, programs, and data owned by individual users should be considered private, whether or not the information is accessible by other users. The Electronic Communications Privacy Act places electronic mail in the same category as messages delivered by the US Postal Service. Tampering with email, interfering with or intercepting its delivery, and using email for criminal purposes may be felony offenses. See the second paragraph of Procedures for further information about privacy.

3. Respect the Rights of Others to Make Use of These Resources

a. placing obscene or harassing material in areas that can be/are publicly accessed;

b. sending/forwarding chain letters or deliberately flooding a user with automatically generated mail;

c. printing or sending excessive copies of documents, files, data, or programs;

d. unauthorized attempts to modify or remove computer equipment;

e. attempting to degrade or disrupt system security or performance;

f. damaging or vandalizing college computing facilities, equipment, software, or computer files.

4. Respect Appropriate Copyright Laws, Licenses, Confidentiality, and Trade Secret Agreements

Much of the software and data that resides on the college's computer facilities is protected by copyright laws and license agreements and may not be copied from, into, or by using campus computing facilities, except as permitted by law or by license from the owner of the copyright. The number of copies and distribution of the copies may not be done in such a way that the number of simultaneous users exceeds the number allowed.

5. Obey Established Guidelines for any Networks or Systems Used Inside or Outside the college

Accessing computers, software, data or information, or networks without proper authorization using college equipment, a college account, or the college network, regardless of whether any damage is done or whether the computer, software, data, information, or network in question is owned by the college, will be treated as an abuse of your Silver Lake College computing privileges. Violating guidelines of non-college networks or systems, even if using non-college resources, may be grounds for revocation or suspension of college computing privileges.

6. System Administrators

In addition to the rules outlined above, system administrators must take reasonable and appropriate steps to see that all license agreements are faithfully executed on all systems, networks, and servers for which they have responsibility. They must take reasonable precautions to guard against corruption of data or software, damage to hardware or facilities of the college, and illegal copying of college software. They must implement college policies as related to these computer systems and must treat information about and information stored by the system's users as confidential.

Anyone authorized to add or delete files from a hard drive of a college computer that is regularly available to more than one individual is acting as a system administrator. System administrators are those who perform functions on college computer equipment including, but not limited to, installing hardware and software, managing a computer or network, and keeping a computer operational.

In the normal course of working with the college's networks and computers, the staff responsible for maintaining those systems may come across and see information stored on college-owned equipment, as well as on personnel equipment that is connected to the college network. Unless there are suspected violations of law or college policy, the staff shall respect the privacy of the individual. Should the faculty or staff member overseeing these systems suspect such violations, the procedures of the next section shall apply.

7. Procedures When Abuse/Misuse is Suspected

When there is an indication that misuse has occurred, the alleged offense is to be reported immediately to the Chief Information Officer and to the appropriate member of senior staff. If there is reason to believe a person's safety is at risk, Safety and Security will also be notified. Information Technology and the appropriate senior staff member shall investigate the incident and may restrict a user's computing privileges.

If an emergency entry is urgently needed to preserve the integrity of facilities or to preserve public health and safety, Information Technology (IT) staff may access files or computer components on, or attached to, the college network without the consent of the user. The college, through the Chief Information Officer, will log all instances of investigative access without consent. Faculty or staff overseeing the college's network servers will also log any emergency entry within their control for subsequent review as soon as possible by the President or appropriate Vice President.

When an alleged offense is reported, Information Technology may make copies of the alleged offender's files to preserve evidence. In order to preserve privacy, staff may not access or read any copied files without authorization from the appropriate senior administrator.

Some instances in which computer resources are used inappropriately may lead to disciplinary action in two different venues (e.g., computer-assisted plagiarism, such as copying a computer file and using it as a model or submitting it as your own work without attribution, could result in disciplinary action according to Academic Honesty guidelines as well as this policy).

Disciplinary action may include loss of computing privileges and other sanctions up to and including non-reappointment, discharge, and/or dismissal. Alleged student misuses will be handled according to the college's judicial system procedures. Alleged faculty misuses will be handled according to the college's procedures for evaluation, termination, or non-renewal. If the alleged misuse by a member of the

faculty or staff involves harassment, it will be handled according to the procedures in the policy on personal harassment.

Abusers of the college's computing resources may also be liable for civil or criminal prosecution. It should be understood that nothing in this policy can preclude enforcement under federal, state, and local laws and regulations.

Policies on Silver Lake College Computer Accounts

Silver Lake College computer accounts are offered at no charge to all students, staff, and faculty of Silver Lake College. One can access these accounts via the network in computer labs, classrooms, all residence hall rooms, faculty/staff offices, or by remote authentication. Each account offers access to the Internet, e-mail, and file storage.

Account Access

New students obtain their accounts either through the admissions process or during orientation. Accounts may also be obtained throughout the semester in the IT office during posted hours. Student accounts are closed after graduation and archived up to one year before removal.

Faculty and staff obtain an account by contacting the IT Office. Depending on the circumstances, faculty and staff accounts may be obtained before or after the person's employment start date. Accounts will be closed upon termination of employment. Depending on the circumstances, full accounts or forwarding may be maintained for a specified period of time after employment termination with written (or email) authorization from the appropriate Vice President.

Privacy and the Internet

Silver Lake College respects freedom of expression and the existence of an open environment conducive to inquiry and learning in the use of its computing resources. The college respects the privacy of the members of the college community - faculty, staff, and students. Correspondingly, by sharing and using the information technology resources of the college, information technology users accept full responsibility for their actions and agree that they will use these resources in an ethical manner. This policy should be read and interpreted in conjunction with other Silver Lake College policies including but not limited to policies prohibiting harassment, discrimination, offensive conduct or inappropriate behavior.

While the college will attempt to safeguard privacy of information stored in user accounts, or on other Silver Lake College owned computer resources (such as departmental servers), the college cannot guarantee that privacy will be absolute. By its nature, electronic communication leaves records or logs of information that can be used to trace problems. Some of these logs are, by the nature of the systems, subject to review by any user of certain systems. Transmitted

information, such as e-mail messages, can easily be forwarded and copied by recipients, and can (with specialized equipment) be read in transit. Personal systems attached to the network may have all or part of their data publicly available. Even data that are password-protected may be available if the password is too easily "hacked." Files stored on IT servers and on some other college servers are backed up regularly. This means that information deleted by an individual may continue to be accessible in some form.

While recognizing the critical importance of privacy in an academic setting, the college may determine that certain broader concerns outweigh a user's expectation of privacy and warrant college access, through carefully prescribed processes, to the relevant information technology systems without the consent of the user. Those circumstances are discussed below, together with the procedural safeguards established to ensure access is gained only when appropriate.

The college does not, as a rule, monitor the content of materials transported over the college's network resources or posted on college-owned computers and networks but reserves the right to do so. The college reserves the right to copy and examine any files or information residing on college systems allegedly related to unacceptable use. It also reserves the right to protect its network from systems and events that threaten or degrade operations.

In accordance with state and federal law, the College may access all aspects of its information technology systems, without the consent of the user, in the following circumstances:

- When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the college's information technology system;
- When such access to information technology systems is required to carry out essential business functions of the college;
- When required by federal, state, or local law or administrative rules;
- In connection with the preservation of public health and safety; or
- When there are reasonable grounds to believe that a violation of law or a significant breach of college policy may have taken place and access or inspection or monitoring may produce evidence related to the misconduct.

In the normal course of working with the college's networks and computers (e.g., routine maintenance, replacing a hard drive, analyzing abnormally high usage of the network), the staff responsible for maintaining those systems may come across and see information stored on college-owned equipment, as well as on personal equipment that is connected to the college network. Unless there are suspected violations of law or college policy, the staff will respect the privacy of the individual. Should the faculty or staff member overseeing these systems suspect such violations, the following procedures will apply:

- Investigative access without the consent of the user will occur only with the approval of the Dean of the College (for faculty and academic staff users), the Director of Human Resources and Risk (for staff users), the Dean of Students (for

student users), the President (for senior staff), or their respective appointees, except when an emergency entry is urgently needed to preserve the integrity of facilities or to preserve public health and safety. The college, through the Chief Information Officer, will log all instances of investigative access without consent. Faculty or staff overseeing the college's network servers will also log any emergency entry within their control for subsequent review, as soon as possible, by the President, the Dean of the College, the Director of Human Resources and Risk, or the Dean of Students.

- A judicial or investigatory proceeding on the part of the college, or legal investigation backed by a specifically-targeted court order, may require reading or relinquishing a personal file.
- The results of such monitoring, including the contents and records of individual communications, may be made available to appropriate college personnel or law enforcement agencies and may be used in appropriate college disciplinary proceedings.
- Communications made by means of the college's computing resources are also subject to Wisconsin's Public Records Statute.
- Inspection of files under these circumstances is limited to the least invasive degree of inspection required to perform the required work. The affected individual will be notified of the actions taken at the earliest possible opportunity that is lawful and consistent with other college policy.
- If the actions of computer-related hardware or software threaten the soundness, stability, functionality, or technical integrity of the Silver Lake College intranet, or other computer resources on that intranet, then the college staff has the authority to immediately disconnect that component from the intranet, but must then immediately begin an investigation using the procedures outlined above.

The policies above apply to faculty, staff, or student employees of the college who are acting in the capacity of a server administrator. Anyone authorized to add or delete permanent files from a hard drive of a college computer that is regularly available to more than one individual is acting as a system administrator.

Because the college is the owner of all information technology resources provided by the college to users, the college reserves the right to deny use to those who have used them in an irresponsible manner. The college may deactivate a user's privileges, whether or not the user is suspected of any violation of this policy, when necessary to preserve the integrity of facilities, user services, or data.

By connecting privately owned personal computers or other information technology resources to the college's network, users consent to the college's use of monitoring and scanning programs (e.g., a network port scanning program) for security purposes on those resources while attached to the network.

Portions of this policy apply to any student, faculty, or staff using the Silver Lake College network, regardless of whether they maintain a Silver Lake College computer account. For individuals requesting a Silver Lake College computer account, IT is authorized to attach to the policy above the consent form below and require that individual to sign the form acknowledging those polices before they receive their account.