Policy Title	Effective Date	Policy Number
Computer Use Policy for Students	07/2002	SS-045
Responsible College Division/Department	**Responsible College Manager Title**	
Student Services	Student Services Manager	

Policy Statement

I. INTRODUCTION

The computing and telecommunicating networks, computing equipment and computing resources of Lakeshore Technical College (hereinafter "College") are owned by the College and are provided primarily to support the academic, administrative, and business functions of the College. Additional rules and regulations may be adopted by various divisions/departments to meet specific administrative or academic needs.

Any adopted requirements must be in compliance with applicable federal and state laws, and this policy.

II. REGULATORY LIMITATIONS

A. Without prior notice, the College may monitor use of the equipment and networking structures and all systems for legitimate academic, administrative, and business reasons, including:

1. To ensure the security and operating performance of systems and networks.

2. To ensure appropriate academic, administrative, business and incidental personal use of equipment/materials.

3. To enforce College policies.

Monitoring includes the right of the College to access messages and files which have been deleted, but not fully erased from systems. Legitimate academic, administrative, or business reasons include, but are not limited to, the right to inspect the contents of electronic messages or files in the course of an investigation prompted by evidence of violation of a College policy or as necessary to locate substantive information which is not readily available through other means. The contents of electronic communications files and records obtained for legitimate academic, administrative or business needs may be disclosed within the College District, without the permission of student, to those with an essential need to know, as well as to law enforcement and regulatory agencies.

Notwithstanding the right of the College to view, retrieve, and read any and all electronic messages, records, or files within College systems; electronic messages, records and files must otherwise be treated as confidential by students and accessed only by the author or intended recipient. Students may not attempt to gain access to another person's electronic messages, records, or files without authorization or the permission of the person.

B. The College reserves the right to limit access to all equipment, networks, and resources

when federal or state laws or College policies are violated, or when College contractual obligations or College operations may be impeded.

C. The College may authorize confidential passwords or other secure entry identification; however, students are to have no expectation of privacy in the material sent or received by them over the College computing systems or networks. While general content review will ordinarily not be undertaken, monitoring of this material may occur for the reasons specified above.

   Computer passwords are not, and are not intended as a guarantee of confidentiality or privacy. Students may not use a password, access a file, or retrieve any stored information unless authorized to do so.

   Each individual user is responsible for the proper use of his/her assigned account, including password security. Users must not share computer accounts or disclose access information to unauthorized persons.

D. The College generally does not monitor or restrict material located in College computers housed within a private domicile or on non-college computers, whether or not such computers are attached or able to connect to campus networks.

E. All material prepared and used for purposes and posted to or sent over College computing and other telecommunicating equipment, systems or networks must be accurate and must correctly identify the author and receiver.

F. No person shall make illegal copies of software. Illegal copies of software may not be run on any District computer. The Information Technology staff will take the necessary action to prevent violations of this requirement. Students are responsible for any and all liability resulting from violation of this prohibition.

G. The College is not responsible for the loss of data or interference with files which may occur in the course of maintenance of networks or equipment.

H. The College is not responsible for lost or deleted files which have been saved on disks.

III. PERMISSIBLE USE

Students are required to adhere to this policy and any related College rules, regulations and procedures for work produced on computing equipment, systems and networks. Students may access these technologies for academic, administrative, business and incidental personal uses, if the following restrictions are followed:

A. The use is lawful under federal or state law.

B. The use is not prohibited by Lakeshore Technical College District Board, College, or institutional policies.

C. The use does not damage or overload College computing equipment or systems, or

otherwise harm or negatively impact the systems' performance.

D. The use does not contravene copyright or trademark law.

E. The use does not result in commercial gain or private profit (other than as allowable under College intellectual property policies).

F. The use does not state or imply College sponsorship or endorsement.

G. The use does not violate state or federal laws or College policies against race or sex discrimination, including, but not limited to, racial slurs, gender specific comments, comments on sexual orientation or sexual harassment.

H. The use does not involve unauthorized passwords, identifying data, or any other action that attempts to circumvent, disable or overload system security, or in any way attempts to gain unauthorized access.

I. The use does not involve activities which interfere with or disrupt network users, services or equipment, to include, but not limited to:

   a. Distribution of unsolicited advertising or mass mailings;

   b. Propagation of computer worms or viruses; and

   c. Downloading and/or running any destructive or disruptive programs on College computer systems.

J. The use does not involve accessing or attempting to access by "hacking" or any other unauthorized entry, materials, information, resources, communication devices, or the files of other users, which the student reasonably understands to be restricted to persons other than the student. Intentional interception of any electronic communication is considered unauthorized access and may violate the Electronic Communications Privacy Act.

K. The use does not involve in any manner disabling or inactivating virus scanning software or restrictive filters.

IV. ILLEGAL ACTIVITY

A. Any illegal use of the network, or its use in support of such activities, is strictly prohibited. Illegal activities are defined as a violation of local, state, and/or federal laws.

B. The submission, publication or transmission of information or data of any type for the purpose of planning, preparing or engaging in criminal activity of any type is strictly prohibited.

C. College officials will report actual or suspected criminal conduct to law enforcement authorities.

V. VIEWING OR DISTRIBUTING OBSCENE OR PORNOGRAPHIC MATERIALS

A. Students may not intentionally access, download, store, or transmit obscene or pornographic sites, materials, files or messages through the College District Information Systems or using any College District computing and telecommunicating networks, equipment or computing resources to include, but not limited to, any sites, materials, messages, or files, which:

1. Contain adult oriented or pornographic images, written materials, or discussions;

2. Are restricted to adults or persons age 21 or over because of adult oriented sexual or violent content;

3. Contain sexually explicit images or materials of any type, to include images of the human body which depict nudity or sexual excitement, as well as actual or simulated sexual acts.

Conduct of this character is not, and will not be recognized as appropriate or authorized use of College computing equipment, information systems and networks for personal, academic, administrative, or business purposes.

B. Violation of the foregoing section IV., A., of this policy will result in disciplinary action under section VI., below.

VI. SUSPENSION OF PRIVILEGES BY MANAGER OF STUDENT SERVICES OPERATIONS

A. The College's Manager of Student Services Operations may suspend a student's access privileges for as long as necessary to protect the College's computing resources. As soon as practicable following the suspension, the Manager of Student Services Operations must take the following actions:

1. The student must be provided with notice of the computing resources suspension and the reasons for it.

2. The student must be given an opportunity to meet with the Manager of Student Services Operations to discuss the suspension if the student requests it.

3. Following the meeting, the student must be notified that the student may appeal to the Manager of Student Services Operations' immediate supervisor if the student is dissatisfied with the outcome of the meeting.

B. The Manager of Student Services Operations may refer the matter for action under the student code of conduct.

VII. VIOLATION OF POLICY

A. Any violation of this policy will be considered “misconduct” under the College student code of conduct and the offending student will be subject to the process as outlined.

Violations should be reported as provided under the code.

B. Sanctions for violation of this policy may include a revocation or suspension of access privileges in addition to the sanction provided under the student code of conduct.

C. Violations of federal or state law may be referred for criminal or civil prosecution.

D. Disciplinary decisions will be based upon, but will not be limited to, the following:

1. The nature of the misconduct, to include the character of materials, files, messages or sites, created, accessed, sent, viewed, or damaged.
2. The frequency with which unauthorized materials, files, sites or messages were accessed, downloaded, stored, transmitted, or damaged.
3. The time of day during which the conduct occurred.
4. Whether other persons were involved in any way, either voluntarily or involuntarily.
5. Whether the conduct is subject to criminal prosecution.
6. Whether the conduct has resulted in a complaint by another person.
7. Impact upon other students.
8. Prior disciplinary record.
9. Cost incurred by the College.

E. Unauthorized or improper use of a student account, password, or access information will not excuse the student from disciplinary action, if the student failed to comply with the requirements of this policy regarding network security.

VIII. APPLICATION OF PUBLIC RECORDS LAW

All information created or received for work purposes and contained in College computing equipment files, servers, or electronic mail (email) depositories are public records and are available to the public unless an exception to the Wisconsin Public Records Law applies. This information may be purged and destroyed only in accordance with the College records retention schedule.

Reason for Policy

The use of this equipment and technologies is governed by federal and state law, and College policies and procedures.

Cross References and Legal Review

Created/Adopted: 7/2002
Reviewed/Revised: 04/01/06
Legal Reference:
Cross Reference: Student Conduct, Student Discipline, Microcomputer Software Protection, Material Resources Management, American with Disabilities Act, Equal Opportunity and Affirmative Action

Legal Counsel Review and Approval:
Board Policy: III.A. General Executive Constraint, III.B. People Treatment, III.F. Asset Protection

Definitions