PC Network/Internet Acceptable Usage Policy

Introduction

The College owns and operates a variety of computing systems which are provided for the use of College students, faculty, and staff in support of the programs of the College and are to be used for education, academic development, and public service only. Commercial uses are specifically excluded. All students, faculty and staff are responsible for seeing that these computing facilities are used in an effective, efficient, ethical, and lawful manner.

These regulations establish rules and prohibitions that define acceptable use of these systems. Unacceptable use is prohibited, and is grounds for loss of computing privileges, as well as discipline or legal sanctions under Federal, State, and local law.

Statement of Policy

A. Audience and Agreement

1. All users of the College computing systems must read, understand, and comply with the policies outlined in this document, as well as any additional guidelines established by the administrators (AS400 and PC Network) of each system. Such guidelines will be reviewed by the College and may become subject to approval as a college policy or procedure.
2. By using any of these systems, users agree that they will comply with these policies.

B. Rights

1. These computer systems, facilities, and accounts are owned and operated by the College. The College reserves all rights, including termination of service without notice, to the computing resources that it owns and operates. These procedures shall not be construed as a waiver of any rights of the College, nor shall they conflict with applicable acts of Law.
2. Users have rights that may be protected by federal, state, and local law.

C. Privileges

1. Access and privileges on College computing systems are assigned and managed by the appropriate system administrator. Eligible individuals may become authorized users of a system and be granted appropriate access and privileges by following the approval steps prescribed for that system.
2. Faculty/staff and students may use a lab at any time the facility is not in use. If the lab is in use the permission of the instructor should be obtained. A faculty/staff member or a student should not use a lab if the use monopolizes equipment or disrupts the scheduled use of the facility.
3. Faculty making assignments requiring students to use a computer (other than classes already scheduled) must make arrangements with the appropriate system administrator

D. Responsibilities

1. Users are responsible for maintaining the following:
    - a) An environment in which access to all College computing resources are shared equitably among users:
    - b) The system administrator of each system sets minimum guidelines within which users must conduct their activities.
2. An environment conducive to learning:
    - a) A user, who uses the College's computing systems to harass, or make defamatory remarks, shall bear full responsibility for his or her actions. Further, by using these systems, users agree that individuals who transmit such remarks shall bear sole responsibility for their actions. Users agree that the College's role in managing this system is only as an information carrier, and that they will never consider transmission through this system as an endorsement of said transmission by the College.

- b) Many of the College computing systems provide access to outside networks both public and private which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users are further advised that the College does not assume responsibility for the contents of any of these outside networks.
- c) The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through College systems.
- d) Further, the user agrees to follow proper etiquette on outside networks. Documents regarding etiquette are available through system administrators and through specific individual networks.
- e) The user agrees never to attempt to transmit, or cause to be transmitted, any message in which the origination is deliberately misleading.
- f) The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origination, the person who performed the transmission will be solely accountable for the message, not the College, which is acting solely as the information carrier.

3. An environment free of illegal or malicious acts:
   - a) The user agrees never to use a system to perform an illegal or malicious act. Any attempt to increase the level of access to which (s)he is authorized, or any attempt to deprive other authorized users of resources or access to any College computer system shall be regarded as malicious, and may be treated as an illegal act.
4. A secure environment:
   - a) Any user who finds a possible security lapse on any system is obliged to report it to the system administrators. The system must not be used until the system administrator has investigated the problem.
   - b) Knowledge of passwords or of loopholes in computer security systems shall not be used to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources or otherwise make use of computing resources for which proper authorization has not been given.
   - c) Users are responsible for backup of their own data.

E. Accounts

1. All accounts allowing access to the College computer resources must approve by the appropriate system administrator including the issuing of passwords.
2. In the event an individual is no longer employed by the College it is the responsibility of the employee's supervisor to notify the appropriate system administrator to close the former employee's account.
3. Users may not, under any circumstances, transfer or confer these privileges to other individuals. Others shall not use any account assigned to an individual without written permission from the system's administrator. The authorized user is responsible for the proper use of the system, including any password protection.

F. Confidentiality

The College reserves the right to access all information stored on College computers without notice. File owners will be notified of file access and/or maintenance, in advance, if such notice is practical. When performing maintenance, every effort is made to insure the privacy of a user's files. However, if policy violations are discovered, they will be reported immediately to the appropriate systems administrator.

G. System Usage

Electronic communications facilities (such as e-mail) are for College related activities only. Fraudulent, harassing or obscene messages and/or materials are not to be sent or stored.

H. System Performance

No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any College computer system.

I. Unauthorized Access

No one should deliberately attempt to degrade the performance of a computer system or to deprive authorized personnel of resources or access to any College computer system.

J. Copyright

Computer software protected by copyright is not to be copied from, into, or by using campus computing facilities, except as permitted by law or by the contract with the owner of the copyright.

Peer-to-Peer file sharing is prohibited by Northwest-Shoals Community College

College networks and equipment may not be used to violate copyright laws. The unauthorized reproduction of copyrighted materials, including illegal downloading or sharing of copy righted music, movies, books, etc., is a serious violation of NW-SCC's Network Usage Policy as well as U.S. Copyright Laws.

Summary of Civil and Criminal Penalties for violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense.

For more information, please see the Web site of the U.S. Copyright Office at www.copyright.gov, especially their FAQ's at www.copyright.gov/help/faq.

K. Violations

Appropriate disciplinary action will be taken against individuals found to have engaged in prohibited use of the College AS400 or PC network/internet resources. The following sanctions could be imposed for a violation of any of the policies and procedures stated herein.

1. Immediate loss of access.
2. Additional disciplinary action to be determined by the college in line with existing policies.
3. Legal action, when applicable.

L. Additional Guidelines

System administrators will establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines will cover such issues as allowable connect time and disk space, handling of irretrievable mail, responsibility for account approval and other items related to administering the system.