

CSN POLICY: Information Systems and Electronic Resources Acceptable Use Policy

Approved: Michael D. Richards
CSN President

May 27, 2008
Date

Faculty Senate Recommendation

Recommended X Not Recommended __

Judy Stewart
Faculty Senate Chair

May 9, 2008
Date

Contents:

1. POLICY PURPOSE AND BACKGROUND
2. POLICY STATEMENT
3. AUTHORITY AND CROSS REFERENCES
4. KNOWLEDGE OF THIS POLICY
5. DEFINITIONS
6. RESPONSIBILITIES
7. EXCEPTIONS
8. CONTACT
9. HISTORY

1. POLICY PURPOSE AND BACKGROUND

Information technology systems and electronic resources are provided to the members of the College of Southern Nevada (CSN) community with the understanding that they will use them with mutual respect, cooperation and collaboration, and in compliance with all applicable policies, laws and regulations.

These resources are finite but their usage is growing and expanding; the resources must be shared generally and as with any interconnection of electronic resources, one individual can have a dramatic effect on others within the network. Therefore, the use of the CSN network and electronic resources is a revocable privilege.

All constituents will benefit if all users of the CSN electronic systems avoid any activities which cause problems for other users. CSN reserves the right to monitor, limit, and restrict electronic messages, network/systems traffic, and the public or private information stored on computers owned, maintained, or managed by CSN. Anyone who uses computers not owned, maintained, or managed by CSN that abuse campus services may also be denied access to campus resources. Email/voice mail, web pages, and digital content are subject to archiving, monitoring, or review, and/or disclosure by other than the intended recipient as provided in NSHE Board of Regents' Handbook, Title 4, Chapter 1, Section 22, "Privacy Issues".

CSN requires that anyone using CSN's information technology systems or electronic resources abide by the following policy:

2. POLICY STATEMENT

CSN requires access to its information technology systems and electronic resources (hereinafter

"Systems") to be authorized and pre-approved, and that users understand that laws currently exist that prohibit the following:

- Electronic libeling or defamation
- Sending/Posting/Broadcasting messages that incite hate or violence
- Transmitting repeated unwanted personal advances
- Falsifying information or impersonation
- Unauthorized use of, providing, or copying of protected intellectual or copyrighted property

CSN's network is a private network separate and distinct from the public Internet. Therefore, access to and use of CSN's network must comply with all CSN's policies, rules and regulations and with all local, state, and federal laws. Examples of prohibited activities outside of prescribed course related activities include but are not limited to:

- Posting or transmission of confidential information
- Use of offensive or discriminatory language
- Transmission or display of graphic images, sounds or text that is sexual or offensive in nature
- Unauthorized use of other's passwords or accounts
- Use of the Systems for personal profit or gain
- Use of the Systems to harass, threaten, or otherwise invade the privacy of others
- The installation or use of any servers on the network not expressly approved by the Office of Technology Services (hereafter "OTS")
- Deliberate attempts to cause breaches of the network, servers, telecommunications systems or security or to examine network traffic
- Initiation of activities which unduly consume computing or network resources
- Use of applications, for example P2P, to receive and/or distribute copyrighted materials, such as movies, music, and video
- Tampering with computer files, software, or knowingly introducing a virus or malicious code to the to the CSN systems
- Unauthorized changes to the CSN web pages
- Playing games in CSN computer labs for entertainment
- Excessive use of network bandwidth, storage, and any computer resources for purposes unrelated to College activities

Each user is responsible for the security of his/her own account, password, and any workstation to which they are logged in. A complex and securely guarded password provides a high level of assurance of privacy and security of resources; all users are responsible to change their password as recommended by OTS. A password is not to be shared with others or posted in a place accessible by others. A password authenticates the holder as an authorized user of the Systems and must be protected from all others.

Users must understand that email is not absolutely private and should practice caution in sending messages that a user would not want everyone to see. OTS does not make a practice of monitoring email and other files. When there is a suspected violation, CSN reserves the right to examine material stored on or transmitted through its Systems in accordance with NSHE Board of Regents' Handbook, Title 4, Chapter 1.

CSN and users of its Systems must comply with the copyright protection given by international agreements and federal law to owners of software and intellectual property under the United States copyright laws, including but not limited to the Copyright Act of 1976 and the Federal Digital Millennium Copyright Act of 1998, and including the restrictions that apply to the reproduction of software and intellectual property. Users of the Systems must ensure that the bounds of permissible copying under the fair use doctrine are not exceeded (i.e., a backup copy may be made). It is against the law to copy or reproduce any licensed software or intellectual property, or to download from the Internet any copyrighted material, including fonts, music, movies, and videos without permission of the copyright

holder and any illegal activity will be dealt with as outlined below as well as expose the user to criminal charges. No one may use software that has been obtained illegally on the CSN Systems or on personal equipment used at CSN. Violation of these requirements will subject the offender to disciplinary action at CSN as outlined below, as well as expose the user to accountability in a court of law.

While computer equipment and access to the Systems is provided for CSN work and education purposes, incidental personal use is permitted as long as it is not inconsistent with this Policy and it doesn't interfere with employment and education responsibilities.

Eating and drinking is not permitted in the immediate area of any computer in open labs and classrooms.

Violations

In addition to liability and penalties that may be imposed under federal, state or local laws, users of the Systems who fail to fulfill their responsibilities and engage in prohibited conduct may be subject to disciplinary action. CSN may restrict or suspend user privileges while the alleged violation(s) are being investigated and disciplinary action pursued. Disciplinary action shall be taken by the Vice President of Student Affairs relative to student violations, and by the appropriate CSN officer relative to faculty, staff, and/or CSN affiliate violations. A violation may also result in a referral to law enforcement authorities.

In accordance with CSN and NSHE policies and state and federal laws, OTS may monitor the CSN Network for activity which violates this Acceptable Use Policy.

3. AUTHORITY AND CROSS REFERENCES

The basis for this policy is provided in the following:

- Nevada Constitution Article 11
- Nevada Revised Statutes sections 197.110 (2) and 205.473 through 205.513
- Board of Regents Handbook Title 4, Chapter 1, Section 22
- Board of Regents Handbook Title 2, Chapter 6 et al
- CSN Student Conduct Code
- "Student Rights and Responsibilities" section of the Student Handbook

4. KNOWLEDGE OF THIS POLICY

CSN expects that all individuals including, but not limited to, CSN students, faculty, and staff using its Systems will abide by the Acceptable Use Policy.

5. DEFINITIONS

6. RESPONSIBILITIES

The responsible parties that are not applicable to this particular policy are annotated N/A.

The President:

- Final approval authority
- Implementation

Vice Presidents (List applicable VPs):

- Executive Vice President
- Vice President of Student Affairs
- Vice President of Academic Affairs

- Vice President of Administrative Operations

CSN Faculty Senate:

- Development/revisions
- Recommending authority

CSN Administrative Code Officer:

- Technical changes (nomenclature and verbiage)

Standing Committees:

- Student Conduct Code Appeals

Coordinator:

- Chief Information Officer

7. EXCEPTIONS

The President has the discretion to suspend or rescind all or any part of this policy or related procedure(s) when advised by competent legal authority that this policy or related procedure(s) is wholly or in part in conflict with laws or procedures of a superior governing body. The President shall notify the appropriate CSN personnel of the suspension or rescission and cause any necessary changes to be made to this policy.

8. CONTACT INFORMATION

Direct questions about this policy to the following offices:

Subject	Contact
General questions from institutional personnel	CSN General Counsel
How to write Policies and Procedures	Member of Policies and Procedures Guidance Committee and CSN General Counsel
Specific questions related to the detail	Chief Information Officer (702) 651-5900

9. HISTORY

June, 2007:	Forwarded to President Carpenter bypassing Faculty Senate Review
June 20, 2007:	Approved by President Carpenter without Senate Review
January, 2008:	Forwarded by Faculty Senate Chair to the Ad Hoc Committee on the Use of Online Resources for review
February XX, 2008:	Returned with to Faculty Senate Chair with revisions for approval by Faculty Senate
May 9, 2009	Approved by Faculty Senate
May 27, 2008	Approved by President Richards