BOARD POLICY

The Board of Trustees encourages employee use of computing and telecommunications technology in the performance of job duties in the State College System, especially in those areas involving teaching, instruction, research and public service.

The computing resources and facilities offered by the State Colleges are the property of the State Colleges and are to be used for the sharing of knowledge, the creative process, and collaborative efforts within the State Colleges’ educational, research and public service missions.

The guidelines outlined in this policy are to be followed by all users of the State College Wide Area Network pertaining to the use of communications facilities, equipment and services offered by the State Colleges, and to ensure compliance with applicable laws and regulations.

The provisions expressed in this policy also apply to all users of any other networks that are accessed through a State College connection.

Acceptance of any account code (username/password) that provides access to computing resources and/or to State College information systems shall constitute an agreement on behalf of the user or any other individual accessing such information to abide and be bound by the provisions of this policy. Access to State College information systems is a privilege, not a right. Every user is to be responsible for the integrity of the system, respect the rights of other users, the integrity of the physical facilities and controls, and all pertinent license and contractual agreements related to the college systems.

When State College information systems are functioning properly, a user can expect the files and data he or she generates to be private information, unless the creator of the file or data takes action to reveal it to others. Users should be aware, however, that no information system is completely secure. Persons both within and outside the State College System may find ways to access files. Accordingly, the Board cannot and does not guarantee user privacy and users should be continuously aware of this fact.

Employees will make reasonable efforts to safeguard their account codes and passwords. No employee may allow unauthorized persons access to college data, computing or network resources by sharing their password, except in cases necessary to facilitate computer maintenance and repairs. When any user terminates his or her relations with the college, his or her username and password shall be denied further access to college computing resources as stated in institutional policy generally or upon employment termination.

The State Colleges are to make reasonable efforts to safeguard their computing resources through continuous improvement of both privacy and security of personal and institutional information and campus networks by implementing effective security practices and by creating a climate in which all members of the academic community accept responsibility for protecting campus computing and information systems. It is the policy of the Board that any access controls implemented by a State college be done so with the intent to assure that an appropriate balance exists between the need to protect information resources and the need to allow users appropriate access to data and applications.

The State Colleges are a provider of a means to access information available through electronic information resources. The colleges are not a regulator of the content of the information and take no responsibility for the content of the information, except for that information a college creates itself and those acting on its behalf create. The use of electronic media and software provided for employee use by the Nebraska State Colleges are to be used for college related purposes. Use of computers, software, or other college equipment for personal or commercial financial gain is strictly prohibited unless specifically authorized by the Board.
Personal use of State College information systems, including computing resources and facilities is to be for college-related purposes. Limited personal use of college information systems is permitted so long as such usage conforms with policy, does not interfere with college operations including security of the system, network response time, or a user’s performance of duties as a college employee, and does not result in additional costs or inefficiencies to the college or system.

All users of State College electronic equipment and facilities are expected to respect the privacy of other users and their data, and to respect the legal protection provided by copyright and licensing laws to programs and data. All relevant laws and regulations, including state public records laws, federal copyright laws, and federal privacy laws such as the Family Educational Rights to Privacy Act are to be respected by users. Downloading, distributing and/or displaying any copyrighted material without permission of the copyright owner is strictly prohibited.

Except as hereinafter provided no person may, without the express permission of the person on whose assigned computer(s) or in whose account(s) the file resides, examine or copy any file created by the primary user of the computer. Files made available in public directories may be viewed and/or copied, if not in violation of copyright laws, and computer center personnel, after reasonable attempts to contact users have failed, may delete files from the central computer only in cases where space occupied by those files must be reclaimed for the efficient operation of the system. In addition, to maintain the network campus technical personnel will routinely delete malware and other destructive and unrequested intrusions into information systems (viruses, spyware, etc.,) as they are detected.

Refusal to comply with these provisions and any other Federal, State or local laws that govern any aspects of computer and telecommunications use may result in denial of access to State College information systems or other disciplinary action including suspension or termination of employment. The college may restrict or prohibit the use of its information systems in response to complaints presenting evidence of violations of college policies or state or federal laws. Should a violation or policy abuse occur, the individual who deliberately and with full knowledge committed the violation shall be personally liable for his or her actions.

Users are also expected to respect the integrity of computing systems and shall not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.

To prevent software viruses from infecting State College computers and associated networks and to ensure network integrity and security, and to minimize unnecessary support incidents, it is the policy of the Board that only hardware and software approved in accordance with campus procedures is to be installed on college computers. A college employee with college provided computer training, which shall be available on a regular basis, and who can demonstrate a need to load such hardware or software is required to make advanced written request to the college computing center or appropriate person designated by the college, produce proof of license for any software wishing to be installed, and to seek approval from the college prior to the loading of such hardware or software.

Although it is the policy of the State Colleges not to monitor individual usage of any computing resources, the College, or System Office as appropriate, reserves the right to inspect all electronic files, e-mail or voice mail of any employee, without advance notice or specific permission, for any legitimate business purpose. A legitimate business purpose must be based on reasonable cause and be reasonable in both the inception and scope of the inspection. A legitimate business purpose may include, but not be limited to, inspecting the contents of computer files, e-mail and network communications when it is considered necessary to maintain or protect the integrity, security or functionality of college or other computer resources, to protect the college from liability, when there is reasonable cause to believe that the users have violated this policy or otherwise misused computing resources, when an account appears to be engaged in unusual or unusually excessive activity, and when otherwise required or permitted by law. Anytime that monitoring or inspection of electronic files, e-mail or voice mail is carried out by the College/System Office, full documentation is to be made available to the involved personnel. This documentation should include: reason, time, date, document inspected, result of the inspection, and person authorizing the inspection.
Users of State College computing resources should also be aware that on occasion duly authorized college information systems technical personnel, which may include students employed as technicians, have authority to access individual user files or data in the process of performing repair or maintenance of computing equipment the college deems is reasonably necessary, including the testing of systems in order to ensure adequate storage capacity and performance of college needs.

Information systems technical personnel performing repair or maintenance of computing equipment are prohibited by law from exceeding their authority of access for repair and maintenance purposes or from making any use of individual user files or data for any purpose other than repair and maintenance services performed by them. Except for legally authorized access, technical staff must receive employee permission to download or access the material on an employee’s hard drive as well as receive a student’s written permission to access a student’s educational record.

All personnel are prohibited from copying or using any copyrightable works authored by any employee without express written permission in advance from the copyright owner.

Users of State College computing resources, in accordance with procedures established by the college if the maintenance work cannot be automated, must request maintenance work that is needed. Automated maintenance is to be scheduled at appropriate hours so as to minimize the disruption of an employee’s regular workday activities. System upgrades and scheduled maintenance is to be scheduled and announced in advance. In instances where a computer is unattended and a virus is causing system or network problems and it is not practical or reasonable to secure prior permission from the computer user, technical support personnel may disconnect the network port that supports the computer in question. Web pages created using state college computer resources are considered to be college web pages and are to conform to campus publication standards. Originators of all web pages using information systems associated with the college shall comply with college policy and procedures as well as all federal, state and local laws and regulations, including copyright laws, obscenity laws, laws relating to libel, slander and defamation, and laws relating to piracy of software.

Persons creating a web page are responsible for the accuracy of the information contained in the web page. Content should be reviewed periodically to assure continued accuracy. Web pages should include a phone number or e-mail address of the person to whom questions/comments may be addressed, as well as the most recent revision date.

**PROCEDURE**

Each college and affiliate organization is responsible for employee use of computing and telecommunications technology and for ensuring that its users are familiar with the provisions outlined in this policy.

1) Hardware, software, and network equipment is made available to provide and facilitate communication with other State and Federal agencies, with other entities in the field of education, with clients of the State Colleges, and to facilitate the discharge of other employee duties and responsibilities.

2) Such equipment is available for purposes related to the users duties as an employee of the State College System.

3) Use of State College hardware, software, and network equipment must be consistent with the goals of facilitating and disseminating knowledge and information, encouraging collaborative projects and resource sharing, and aiding technological transfer to the various constituencies of the State Colleges.
The following uses are considered unacceptable, unauthorized and prohibited.

1) Use of the system and any attached network, network device, or network service in a manner that precludes or significantly hampers its use by others.

2) Recreational use of the network shall be prohibited if it significantly hampers the use of the system by others. The installation or playing of computer entertainment games on State College equipment is prohibited unless used as instructional tools, as a means of introducing and motivating students and employees to use new computer systems/applications, and as a means of helping students and employees develop and improve manual dexterity to efficiently use the current generation of desktop computers. Games can also be used to illustrate fundamental concepts of computer science and computer graphic design.

3) Use for for-profit activities, for private or personal business, or for any commercial or personal purpose or advertising is unauthorized unless expressly approved by the Board.

4) To transmit or knowingly receive threatening, obscene or harassing materials, or to use the State College network for illegal purposes.

5) To misrepresent oneself or the College when using the network.

6) To use the network to access information or resources unless permission to do so has been granted by the owners or holders of rights to those resources and information.