Computer Resource and Internet Usage Policy (Fair Use Policy)

Overview This college provides access to the vast information resources of the Internet to students, faculty and staff in their educational endeavors. The facilities that provide access represent a considerable commitment of resources for telecommunications, networking, software, storage, etc. This Internet usage policy is designed to help you understand our expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely.

While we've set forth explicit requirements for Internet usage below, we'd like to start by describing our Internet usage philosophy. First and foremost the Internet for this college is an educational tool, provided to you at significant cost. That means we expect you to use your Internet access primarily for educationally related purposes, i.e., to communicate with students, other college personnel and colleagues, to research relevant topics and obtain useful educational Information (except as outlined below). We insist that you conduct yourself honestly and appropriately on the Internet, and respect the copyrights, software licensing rules, property rights, privacy and prerogatives of others, just as you would in any other business dealings. To be absolutely clear on this point, all existing college policies apply to your conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of college resources, harassment, sexual harassment, information and data security, greviance, disruption of college operations and confidentiality.

Unnecessary or unauthorized Internet usage causes network and server congestion. It slows other users, takes away from work time, consumes supplies, and ties up printers and other shared resources. Unlawful Internet usage may also garner negative publicity for the college and expose the college to significant legal liabilities.

The chats, newsgroups and e-mail on the Internet give each individual Internet user an immense and unprecedented reach to promote the interests of the college. Because of that power, we must take special care to maintain the clarity, consistency and integrity of the mission and objectives of the college. Anything any one employee writes in the course of acting for the college on the Internet could be taken as representing the college's educational posture. That is why we expect you to forego a measure of your individual freedom when you participate in chats or newsgroups on college time, as outlined below.

While our direct connection to the Internet offers a cornucopia of potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. As presented in greater detail below, that may mean preventing machines with sensitive data or applications from connecting to the Internet entirely, or it may mean that certain users must be prevented from using certain Internet features like file transfers. The overriding principle is that security is to be everyone's first concern. College employees and students can be held accountable for any breaches of security or confidentiality.

Certain terms in this policy should be understood expansively to include related concepts. “College” refers to Neosho County Community College. The Director of Technology Services serves as the "CHIEF INFORMATION OFFICER", or "CIO" for the college. “College Network” refers to NCCC computing resources including but not limited to computers, software and information at all NCCC campuses, outreach sites and the virtual college, whether or not owned by NCCC. It shall also refer to any NCCC owned computing resource regardless of location. “Internet Access” refers to any use of a password issued by NCCC to access and use what is commonly referred to as the Internet.

"Document" covers just about any kind of file that can be read on a computer screen as if it were a printed page, including the so-called HTML files read in an Internet browser, any file meant to be accessed by a word processing or desktop publishing program or its viewer, or the files prepared for the Adobe Acrobat reader and other electronic publishing tools. "Graphics" Includes photographs, pictures, animations, movies, or drawings. "Display" includes monitors, flat-panel active or passive matrix displays, monochrome or color LCDs, projectors, televisions and virtual-reality tools.

DETAILED INTERNET POLICY PROVISIONS

A) General

1. NCCC shall have the right to review all files and records and the right to periodically monitor, audit or review network, workstation, Internet and e-mail use on the college network. No employee, student or patron should have any expectation of privacy as to Internet access. Our Technology Services department may review Internet activity and analyze usage patterns, and may choose to perform detailed analysis of the data to assure that the college network and Internet access are devoted to maintaining the highest levels of productivity.

2. Users are prohibited from accessing content that is considered to be pornographic in nature or sites that facilitate social networking determined to be sexually explicit. The NCCC network is actively monitored for inappropriate content and anyone found in violation of these polices is subject to loss of internet privileges and/or removal from the facility. Additionally, sexually explicit or other potentially offensive material may not be archived, stored, distributed, edited or recorded using the college network unless directly related to the user's job or the college's educational activities. It is recognized and understood that access to sexually explicit or other potentially offensive material may be required in pursuit of the individual faculty member's responsibilities. It is further understood that said use of the college network, standing alone, should not invoke disciplinary or other punitive measures except for loss of Internet rights and privileges.

3. It is a violation of college policy to store any document or graphic file using our college network that is not directly related to the user's job or the college's educational activities.

4. The college uses independently supplied software and data to identify Inappropriate or sexually explicit Internet sites. We may block access from within the college network to all such sites that we know of. If you find the college network connected incidentally to a site that contains sexually explicit or offensive material, you must disconnect from that site immediately, regardless of whether that site had been previously deemed acceptable by any screening or rating program.

5. This college network and Internet access must not be used to violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. The college will cooperate with any legitimate law enforcement investigation activity, including production of Internet activity logs, computer network and Internet access information upon proper request.

6. Any software or files downloaded via the Internet into the college network become the property of the college. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.

7. No employee, student or patron may use the college network or Internet access to knowingly download or distribute pirated software or data.

8. No employee, student or patron may use the college network or Internet access to knowingly propagate any virus, worm Trojan horse, or trap-door program code.

9. No employee, student or patron may use the college network or Internet access to knowingly disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user (commonly known as "hacking").

10. Each employee, student or patron using the college network shall identify himself or herself honestly, accurately and completely (including one's college affiliation and function where requested) when participating in chats or newsgroups, or when setting up accounts on outside computer systems.

11. Only those employees or officials who are authorized to speak to the media, to analysts or at public gatherings on behalf of the college may speak/write in the name of the college to any newsgroup or chat room. Other employees may participate in newsgroups or chats in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of this college, the employee must refrain from the unauthorized endorsement or appearance of endorsement by the college of any commercial product or service not sold or serviced by this college.

12. The college retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee In the course of his or her duties.

13. Employees are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential college information, student data, trade secrets, and any other material covered by existing college security policies and procedures. Chats and newsgroups for student and patron use through the college network are strictly limited to educational-related purposes. Chats, newsgroups and e-mail usage may be prohibited by individual departments unless specifically necessary for educationally related activities (i.e. online class chats, etc.).

14. Use of college network or Internet access or other means to commit infractions such as misuse of college assets or resources, sexual harassment, unauthorized public speaking and misappropriation of intellectual property are also prohibited by general college policy and will be governed by the relevant provisions of the Board Policy Handbook.

15. Employees may use the college network for non-educational research or browsing outside of regularly scheduled work hours, provided that all other usage policies are adhered to.

16. Employees using the college network or Internet access must take particular care to understand copyright, trademark, libel, slander and public speech control laws, so that our use of the Internet does not inadvertently violate any laws which might be enforceable against us.

17. Employees, students or patrons using the college network may download only software directly related to the user's job or the college's educational activities, and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of Its license.

18. Employees, students or patrons may not use the college network to knowingly download entertainment software or games, or to play games against opponents over the Internet unless the software is directly related to the college's educational activities.

19. Employees, students or patrons may not use the college network to knowingly download images or videos unless directly related to the user's Job or the college's educational activities.

20. Employees, students or patrons may not upload any software licensed to the college or data owned or licensed by the college without the express authorization of the Chief Information Officer.

21. Minor students and patrons (those under the age of 18) must sign the Internet Use Agreement for Minors, and have parental permission prior to use of college computers with Internet access.

B) Email

1. E-mail users at NCCC have a right to expect reasonable privacy of e-mail messages. This means that no one at NCCC is authorized to read another's e-mail except in one of the following three cases:

- By explicit permission of the e-mail's owner.
- By official request of law enforcement authorities or NCCC Internal Audit.
- In direct conjunction with required maintenance of the e-mail system or user workstation by Technology Services personnel, if it cannot be avoided.

2. The e-mail user must not indiscriminately broadcast messages (spamming).

3. Mailings to an entire population (i.e. NCCC All) should be done very seldom, and should be limited to items that are directly related to the work, business and/or mission of the college.

4. The email system should be used for work-related communications.

5. Do not use the email system in such a way that would disrupt the use of the system by others.

6. It is okay to stay logged into the email system in order to be notified immediately when new mail arrives. However, when you leave your work area, you should either logout or make sure your PC keyboard is locked in order to prevent unauthorized use of your account.

7. The e-mail user is responsible for exercising reasonable diligence in archiving or deleting unneeded messages from the inbox, sent items, and deleted items folders. Technology Services reserves the right to limit the size of all user e-mail resources.

C) Technical

1. User IDs and passwords help maintain Individual accountability for Internet access. Any employee, student or patron that obtains a password or ID for Internet access from the College must keep that password confidential. College policy prohibits the sharing of user IDs or passwords obtained for access to college network and Internet sites.

2. Employees, students or patrons using the college network or Internet access should schedule communications-intensive operations such as large file transfers, video downloads, mass e-mailings and the like for off-peak times.

3. Any file that is downloaded to the college network must be scanned for viruses before it is run or accessed.

D) Security

1. The College has installed an Internet firewall to assure the safety and security of the college's Networks. Any employee, student or patron that attempts to disable, defeat or circumvent any college security facility will be subject to disciplinary actions as outlined in college policy.

2. Files containing sensitive college data that are transferred in any way across the Internet must be encrypted,

3. Only those Internet services and functions with documented educational purposes for this college will be enabled at the Internet firewall.

4. Personnel access shall be limited to only the information required to perform a job (also referred to as “need to know”).

5. The identity of all users on NCCC network shall be authenticated with a password and user-ID code; such that no user will be allowed to use the system without having been positively identified first. All user-ids shall be unique to individual assignees. Passwords shall be a minimum of 6 characters and be required to be changed automatically every 30 days, and should under no circumstance be shared with other individuals. In addition, no user should sign on and allow another individual to use that workstation without first signing off. Users should never leave a signed-on workstation unattended.

6. The work of all persons involved in on-line data input and output will be traceable to such individuals via data base record time stamp, and individual library.

7. Data Input and output operators shall be prohibited from working alone, unless authorized by their appropriate supervisor.

8. All PC hard disk drive should be backed up to diskette or tape on a regular basis. What determines “regular basis” will depend on the individual user and the level of data loss that particular users can accept. Primary users of each machine, to be determined by proximity, are responsible for the backup. If the PC is located in a lab, the applicable division chair (or delegate) will be responsible.

9. The Technology Services department (or delegate) will be responsible for the backup and recovery of all NCCC local area network (LAN) servers. Backup will be done to tape or diskette and will provide for adequate safety in the event of data loss. The Technology Services department will document specific LAN server backup and recovery procedures.

E) Software

1. NCCC licenses the use of its computer software form a variety of outside companies. NCCC does

not own this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it.

2. With regard to use on local area network or on multiple machines, NCCC employees shall use the software only in accordance with the license agreement.

3. With regard to use of on-line computer services, NCCC employees and students shall use the software and access provided through NCCC only in accordance with licensing and use agreements with the service provider, and shall not utilize the service to violate the privacy of any other employee or students, or to obtain or release private or confidential information or records of NCCC, its employees or students.

4. NCCC employees or students learning of any misuse of software or on-line computer services at the college shall notify the Chief Information Officer.

5. NCCC reserves the right to remove any user from the college network or Internet access at any time.

6. NCCC employees learning of any misuse of software or related documentation within the college shall notify their immediate supervisor.

7. The Chief Information Officer shall be responsible to conduct software audits annually to insure compliance with board policy and the US Copyright Law. The Director shall have the right to immediately remove any illegally installed software in accordance with board policy.

8. It will be the responsibility of each PC user to maintain the appropriate software licenses for all software contained on the PC. During the annual software audit, the Technology Services department may require proof of license for any software package located on any machine. Primary users of licenses of multiple license agreement software are responsible for providing copies of licenses materials and documentation to other users, as well as documentation concerning distribution. Software without supported license documentation will be removed immediately from the machine as per board policy.

9. The Technology Services department will be responsible for maintaining license materials for all software contained on the NCCC LAN servers as well as the AS400 network. License materials will be inventoried and stored as per the Technology Services standard manual.

F) Copyright Information

Adapted from "Using Software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community" issued by EDUCOM and ADAPSO, 1992

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution. Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic

community.

Here are some relevant facts:

1. Unauthorized copying of software is illegal. Copyright law protects software authors and publishers, just as patent law protects inventors.
2. Unauthorized copying of software by individuals can harm the entire academic community. If unauthorized copying proliferates on a campus, the institution may incur a legal liability. Also, the institution may find it more difficult to negotiate agreements that would make software more widely and less expensively available to members of the academic community.

3. Unauthorized copying of software can deprive developers of a fair return for their work, increase prices, reduce the level of future support and enhancement, and inhibit the development of new software products.

4. Respect for the intellectual work and property of others has traditionally been essential to the mission of colleges and universities. As members of the academic community, we value the free exchange of ideas. Just as we do not tolerate plagiarism, we do not condone the unauthorized copying of software, including programs, applications, data bases and code.

Classification Of Software:

The restrictions and limitations regarding each classification are different.

Commercial

Commercial software represents the majority of software purchased from software publishers, commercial computer stores, etc. When you buy software, you are actually acquiring a license to use it, not own it. You acquire the license from the company that owns the copyright. The conditions and restrictions of the license agreement vary from program to program and should be read carefully. In general, commercial software licenses stipulate that:

- the software is covered by copyright,
- although one archival copy of the software can be made, the backup copy cannot be used except when the original package fails or is destroyed,

- modifications to the software are not allowed,

- decompiling (i.e. reverse engineering) of the program code is not allowed without the permission of the copyright holder.

Shareware

Shareware software is covered by copyright, as well. When you acquire software under a shareware arrangement, you are actually acquiring a license to use it, not own it. You acquire the license from the individual or company that owns the copyright. The conditions and restrictions of the license agreement vary from program to program and should be read carefully. The copyright holders for

Shareware allow purchasers to make and distribute copies of the software, but demand that if, after testing the software, you adopt it for use, you must pay for it. In general, shareware software licenses stipulate that

- the software is covered by copyright,
- although one archival copy of the software can be made, the backup copy cannot be used except when the original package fails or is destroyed,
- modifications to the software are not allowed,
- decompiling (i.e. reverse engineering) of the program code is not allowed without the permission of the copyright holder, and
- development of new works built upon the package(dervative works) is not allowed without the permission of the copyright holder. Selling software as Shareware is a marketing decision, it does not change the legal requirements with respect to copyright. That means that you can make a single archival copy, but you are obliged to pay for all copies adopted for use.

Freeware

Freeware also is covered by copyright and subject to the conditions defined by the holder of the copyright. The conditions for Freeware are in direct opposition to normal copyright restrictions. In general, Freeware software licenses stipulate that

- the software is covered by copyright,
- copies of the software can be made for both archival and distribution purposes but that distribution cannot be for profit,
- modifications to the software is allowed and encouraged,
- decompiling (i.e reverse engineering) of the program code is allowed without the explicit permission of the copyright holder, and
- development of new works built upon the package (derivative works) is allowed and encouraged with the condition that derivative works must also be designated as Freeware. That means that you cannot take Freeware, modify or extend it, and then sell it as Commercial or Shareware software.

Public Domain

Public Domain software comes into being when the original copyright holder explicitly relinquishes all rights to the software. Since under current copyright law, all intellectual works (including software) are protected as soon as they are committed to a medium, for something to be Public Domain it must be clearly marked as such. Before March 1, 1989, it was assumed that intellectual works were NOT covered by copyright unless the copyright symbol and declaration appeared on the work. With the U.S. adherence to the Berne Convention this presumption has been reversed. Now all works assume copyright protection unless the Public Domain notification is stated. This means that

for Public Domain software

- copyright rights have been relinquished,
- software copies can be made for both archival and distribution purposes with no restrictions as to distribution,
- modifications to the software are allowed,
- decompiling (i.e. reverse engineering) of the program code is allowed, and
- development of new works built upon the package (derivative works) is allowed without on the distribution or use of the derivative work.

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.

A Final Note

Restrictions on the use of software are far from uniform. You should check carefully each piece of software and the accompanying documentation yourself

G) Violations

Alleged violations of the above policy should be reported immediately to the Chief Information Officer. With probable cause, the Chief Information Officer will investigate each reported incident and submit findings to the appropriate administrator. The Chief Information Officer shall have the right to immediately terminate use of computer network and/or Internet access of any employee or student for violation of this policy. Appeals of terminated use of computer network and/or Internet access should be made to the chief academic officer or pursue other due process provisions as outlined in the Board of Trustees Policy Handbook. Violations may also subject the individual to additional disciplinary and/or legal action as provided for in the Board Policy Handbook or

appropriate state or federal statutes.

The Board of Trustees at all times reserves the right to add to, delete from, alter or amend these policies.