

Nebraska Christian College

Network Acceptable Use Policy

A. Guiding Principles

The primary purpose of the Nebraska Christian College's computer network is educational. The network serves as a resource for enriching, teaching and learning objectives. Approved uses of the network are intended to enhance NCC's established curriculum. We are stewards to the gift of technology and God requires accountability in its usage. As a fellowship that yields to the mission of God's ministry with a focus on Christ, Nebraska Christian College expects responsible use of technology by students, faculty and staff in obedience to Biblical ethics, commands, and values.

Nebraska Christian College recognizes the value of providing accessible, affordable, high-quality education through various delivery modes, as such NCC provides the Internet. The Internet can help meet some users' information and research needs, as well as provide valuable reference retrieval through electronic means. Assistance with the use of the Internet is intended to support the needs of students, faculty and staff in order to facilitate the intellectual growth and lifelong learning needs of all users.

The following principles will guide our use of NCC's network.

1. Respect for one another's need for access

Students, faculty and staff who are involved in educational or research activities or the administration thereof should have the highest priority in the use of technology. Their use should not be hindered by others engaged in lower priority activity. NCC is a community where all members should act in their neighbor's best interest.

Not hindering legitimate access also means that faculty, staff and students not waste technological resources. This includes use of the computers, telephones, networks or printers. Using more than your share of resources is not good stewardship to the College network, or to others who share it and excessive use of non-course-work related usage will not be tolerated. It also includes destruction or degradation of any resource, either physically or with software.

Internet file sharing and the use of software enabling file sharing services (i.e. Kazaa, Morpheus, Bear Share, etc.) not only raise ethical and legal issues, but consume extremely large amounts of bandwidth that leaves little available to other members of the community. Therefore, Internet file sharing is expressly forbidden on any system on NCC's network.

Educational use takes priority over recreational or extracurricular use in the computer lab. Students checking email, chatting, playing games or other non-educational activity are expected to yield stations to students who wish to do course-related computer work. Upon completion of your work in the lab, you must logoff of the computer. Failure to do so leaves you responsible for the use of your account by another user, and also leaves the data in your student directory vulnerable.

2. Respect for one another's values and feelings

New technologies often enhance our ability to communicate, and greatly increase the risk of communicating poorly and inappropriately. Communication should illustrate respect for others and a sense of personal integrity. Ephesians 4:29 is applicable here: "Do not let any unwholesome talk come out of your mouths, but only what is helpful for building others up according to their needs, that it may benefit those who listen." Thus, communication that degrades or harasses individuals or groups is unacceptable.

The need to communicate with respect and integrity is particularly important in our contacts with those inside, as well as those outside NCC. Our communications will reflect not only on the College, but also on its Christian mission.

Netiquette is etiquette on the Internet. Since the Internet changes rapidly, its netiquette does too, but it's still usually based a few Golden Rules. Listed below are a few tips to practical communication considerations:

\$ The immediacy and availability of email lend themselves to hastily constructed notes that may not express your feelings accurately or may be dashed off without pausing to consider the impact of your words. Never forget that you are putting words into print and that they can come back to you.

\$ Sarcasm and humor may not be nearly as funny as you intended without the benefit of face-to-face communication, and what you intended as a joke may come off as critical and hurtful.

- \$ Be careful what you say about others. Email is easily forwarded; although it is quite rude to forward personal email without the original author's permission.
- \$ Do not type messages in all capital letters. (CAPITAL LETTERS ARE REGARDED AS SHOUTING!)
- \$ Capitalize words sparingly and only to highlight an important point. Another convention is to use *asterisks* around a word to supply emphasis.
- \$ Keep spam in the kitchen cabinet. Spam is a term that refers to widely spreading an unsolicited message (such as a commercial announcement) in inappropriate places, such as to multiple newsgroups or to an electronic mailing list. Think of spam as electronic junk mail and don't do it.
- \$ Copyright and license agreements apply to e-mail just as they do to print publications.
- \$ One way to show your savvy is to use abbreviations and emoticons. Standard abbreviations are widely used in the Internet community, and emoticons are keyboard-created "faces" with special meanings. Here are a few examples:

BTW - By the way
 FAQ - Frequently Asked Questions
 FYI -For your information
 FWIW - For what it's worth
 IAC - In any case
 IMO - In my opinion
 IMHO - In my humble/honest opinion
 LOL - Laughing out loud
 ROFL - Rolling on the floor laughing
 MOTD - Message of the day
 NBIF - No basis in fact
 NRN - No response necessary
 OTOH - On the other hand
 POV - Point of view
 :) - Happy face to indicate humor
 ;-) - Happy face with a wink
 :-(- Sad face to indicate displeasure

3. Respect for one another's property

Theft or unauthorized use of either tangible property or intellectual property will not be tolerated. This includes unauthorized copying of copyrighted software and any other form of media, which is not only unethical, but also is illegal.

Federal copyright law applies to all forms of information, including electronic communications. Violations of copyright laws include, but are not limited to, making unauthorized copies of any copyrighted material (including software, text, images, audio, and video), and displaying or distributing copyrighted materials over computer networks without the author's permission except as provided in limited form by copyright fair use restrictions. The "fair use" provision of the copyright law allows for limited reproduction and distribution of published works without permission for such purposes as criticism, news reporting, teaching (including multiple copies for classroom use), scholarship, or research.

4. Respect for one another's privacy

Respect for others also means respect for their privacy. Unauthorized reading or altering of someone else's files, email, or other communications is prohibited.

B. Responsible Use Policy Detail

Nebraska Christian College's information systems, including but not limited to computers, voice mail, email and access to the Internet, are provided as tools in support of the mission of NCC. The principal concern of this responsible use policy is the effective and efficient use of Information Technology (IT) resources. Therefore, the primary focus is to ensure that the resources are used in a manner that does not significantly impair or impede their use by others in the pursuit of the mission of the College.

1. Scope

This policy applies to any user (faculty, staff, student or other) of the College's IT resources, whether initiated from on- or off-campus. This includes any telephone, computer and information system or resource, means of access, networks and the data residing thereon.

2. Overview

Telephones, computers and networks can provide access to resources on- and off-campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations as well as conduct themselves in a way that is consistent with Christian life at NCC.

3. Rights

Access to NCC's network including the Internet by faculty, staff and students is a privilege, NOT a right and is extended for the purpose of academic research, completion of class assignments and other pursuits related to the mission of NCC. Users assume all responsibility for their actions when using the NCC network, email and Internet.

4. Personal Responsibility

All users must take responsibility to monitor their use of the Internet, including the sites they visit and the amount of time they spend in chat rooms. If a user begins to believe they have a problem with their use of the Internet, they should make an appointment with the Dean of Students for review.

At the beginning of the school year, each student will be assigned a confidential login, password and email address, allowing them access to NCC email and their own student account on the NCC network. All NCC email accounts should be checked on a regular basis as faculty, staff and other students will use this email address for various communications with the student. Students are also provided a directory with storage on the NCC server (currently 10MB). This directory is only accessible by the individual student to whom it has been assigned and is to be used for storage of class related material. All users of the network will be held accountable for their use of the computer, including any use of any computer located on the NCC network by someone using their login.

Users of the computer lab may not copy, download, install or otherwise modify the system setup or software.

All existing laws (federal, state and local) and NCC regulations and policies apply, including not only laws and regulations that are specific to telephones, computers and networks, but also those that may apply generally to personal conduct. This may also include laws of other states and countries where material is accessed electronically via College IT resources by users within those jurisdictions, or where material originating within those jurisdictions is accessed via College IT resources.

Fraudulent, harassing, pornographic or obscene materials, whether written, aural or visual, are expressly forbidden on any portion of the network, and may not be stored on any college-owned computer, telephone systems or any system connected to the NCC network.

The College reserves the right to limit access to its resources when policies or laws are violated and to monitor routing information of communications across its network services and transaction records residing on College resources. NCC may monitor and restrict the content of material transported across or posted on College systems to preserve network/system integrity, continued service delivery, and to maintain a safe and wholesome Internet environment to all users of the network consistent with its mission.

Specific details are given in Section C below.

C. Policy Provisions

1. Authorized Use

NCC's IT resources are owned by the College, and access is a privilege granted to faculty, staff and students in support of their studies, instruction, duties as employees, official business with the College, and other College-sanctioned activities.

The privilege of using NCC IT resources may not be transferred or extended by members of the College community to outside individuals or groups.

Gaining access to the College's IT resources does not imply the right to use those resources. The College reserves the right to limit, restrict, remove or extend access to and privileges within, material posted on, or communications via its IT resources, consistent with this policy and applicable law, and irrespective of the originating access point.

It is expected that these resources will be used in an effective and efficient manner in support of the mission of the College as authorized by NCC. All other use not consistent with this policy may be considered unauthorized use and

could subject the user to possible civil charges, criminal charges or disciplinary actions.

2. Data Security, Confidentiality and Privacy

NCC users are responsible for ensuring the confidentiality and appropriate use of College data to which they are given access, ensuring the security of the equipment where such information is held or displayed, and abiding by related privacy rights of students, faculty and staff concerning the use and release of personal information, as required by law or existing policies.

For the purposes of this policy, all institutional data is to be considered sensitive and/or confidential. Access to such data is based on an individual's "need to know" and is restricted to uses directly related to assigned duties. Users are responsible for the security of any accounts issued in their name and any institutional data they may retrieve, modify, reproduce or destroy. Disclosure of confidential information to unauthorized persons or entities, or the use of such information for self-interest or advantage, is prohibited. Access to institutional data by unauthorized persons or entities are prohibited.

In general, information stored on College computers is to be considered confidential unless the owner grants explicit permission to other individuals or groups to view that information or intentionally makes it available to the public. However, all users of NCC's IT resources are advised to consider the open nature of information disseminated electronically, and should not assume any degree of privacy or restricted access to such information as it may be intercepted, copied, read, forged, destroyed, or misused by others.

Unless the law provides otherwise, no personal right of privacy exists in any information placed by students or employees on college-owned computers, or transmitted via the college's voice mail or email systems. In the event of a college investigation stemming from a complaint of alleged misconduct, voice mail, email or files may be locked or copied by IT management to prevent destruction and loss of information, and/or the contents may be reviewed.

Email accounts will be deleted once an individual leaves NCC with no known intention of return or continuance date.

All logins, requests for web pages and commands executed by users are recorded in log files that are owned and maintained by Information Technology. This information is monitored and content may be blocked for inappropriate activity and may be the basis for policy enforcement.

Requests for disclosure of confidential information and retention of potential evidence will be honored when approved by authorized College officials or legal authorities, or when required by state or federal law.

3. Network and System Integrity

Activities and behaviors that threaten the integrity of College computer networks or systems are prohibited on both College-owned and privately-owned equipment operated on or through College resources. These activities and behaviors include but are not limited to:

- \$ Interference with or disruption of computer systems and networks and related services, including but not limited to the propagation of computer "worms," "viruses" and "Trojan Horses".
- \$ Intentional or careless acts, processing extremely large amounts of data, or causing extremely high system utilization to the extent that these interfere with network or system performance so that access to networks or information systems by others may be disrupted or substantially degraded. This includes, but is not limited to any local network file sharing, the transfer of large files across the network and any gaming activity, shared (multi-player) or otherwise which degrades the network performance.
- \$ Failure to comply with requests from appropriate College officials to discontinue activities that threaten the operation or integrity of computers, systems or networks.
- \$ Revealing passwords or otherwise permitting use by unauthorized others, by intent or negligence, of personal accounts for computer and network access. Individual password security is the responsibility of each user.

- \$ Unauthorized scanning of computers and networks for security vulnerabilities and unauthorized attempts to circumvent data protection schemes or uncover security loopholes.
- \$ Connecting unauthorized equipment to the campus network or computers.
- \$ Attempting to alter any College computing or network components without authorization or beyond one's level of authority, including but not limited to bridges, routers, hubs, wiring, connections, etc.
- \$ Negligence leading to damage of College electronic information, information technology resources, computing systems or networks.
- \$ Utilizing network or system identification numbers or names that are not assigned for one's specific use on the designated system.
- \$ Using campus resources to gain unauthorized access to any computer system.
- \$ Violating Copyright and Fair Use practices (see section C7).
- \$ Masking the identity of an account or machine.
- \$ Capturing passwords or data on the network not meant for you.
- \$ Modifying or extending NCC network services and wiring beyond the area of their intended use. This applies to all network wiring, hardware and in-room jacks.
- \$ Placing content on web pages which violates this Network Use Policy.

4. Academic Honesty

The College will not tolerate academic cheating or plagiarism in any form. Users of information technology resources are expected to uphold the standards of Nebraska Christian College (see the Student Handbook for specifics).

5. Commercial and Political Activity

Use of the College's information technology resources is strictly prohibited for hosting or serving unauthorized commercial activities, personal or political gain, private business, fundraising, or use otherwise unrelated to the College. This includes soliciting, promoting, selling, marketing or advertising products or services, or reselling College resources.

6. Trademarks and Patents

Unauthorized use of trademarked names or symbols, including NCC's, is prohibited. Where College resources are used, the College retains ownership of all faculty, staff and student inventions and other intellectual property that may be patented, copyrighted, trademarked or licensed for commercial purposes.

7. Electronic Communications

College electronic communications are to be used to enhance and facilitate teaching, learning, scholarly research, support academic experiences, and to facilitate the effective business and administrative processes of the College.

The following activities and behaviors are prohibited on College or privately-owned equipment or networks operated on College resources:

- \$ Online gambling and file sharing and the use of any media enabling these types of activities.
- \$ Altering electronic communications to hide one's identity or to impersonate another individual. All email, news posts or any other form of electronic communication must contain the sender's real name and/or user ID.
- \$ Initiating or forwarding electronic "chain letters".
- \$ Sending unsolicited commercial advertisements or solicitations.
- \$ Operating unofficial email reflectors.
- \$ Sending messages to large numbers of users.
- \$ Use of system aliases by non-authorized personnel.
- \$ Use of official aliases to broadcast unofficial and/or unauthorized messages.
- \$ Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit permission of the owner.

The College reserves the right to send electronic communications, including large group or broadcast messages, to its own users.

The College reserves the right to limit the size of individual messages being transmitted through College resources.

8. Internet

The College reserves the right to block categories of Internet content as well as specific sites. Currently the College blocks Internet sites that are known to be pornographic, that facilitate the practice of plagiarism, or that provide file sharing services.

D. Consequences of Non-Compliance

1. College

An individual's computer use and/or network connection privileges may be suspended immediately upon the discovery of a possible violation of these policies. Because of the nature of the networking, Information Technology may not know who owns a computer that may be involved in a violation. In this case, access to the network from that computer will be suspended until the owner of the computer contacts Information Technology and resolves the issue.

The Information Technology administrative staff will judge an offense as either major or minor. The Information Technology administrative staff will normally deal with a first minor offense. Additional offenses will be regarded as major offenses. Substantiated, major violations by students will be confidentially reported to the Dean of Students; those of faculty and staff to the President.

Violations of these policies will be dealt with in the same manner as violations of other college policies and may result in disciplinary review.

2. Civil and Criminal

In addition to the above, certain inappropriate use of Information Technology resources may result in personal criminal and/or civil liability.

User shall indemnify NCC for any losses, costs or damages, including reasonable attorney fees incurred by NCC relating to, or arising out of, any breach of this Use Policy by user.

E. Reporting Irresponsible or Inappropriate Use

Suspected violations of this policy should be reported to the Director of Information Technology.

Information Technology personnel will advise the user on what if any action to take, act directly when appropriate, and/or refer the violation to other offices for further action. IT personnel will also assist other offices with investigations of suspected policy violations when appropriate. Information Technology personnel may also be contacted to report violations when the complainant is unable, or it is not desirable, to do so through other channels.

F. Fees

A listing of student fees for use of IT resources is available upon request.

G. Exceptions

Anyone desiring an exception to this policy must get written approval from the Director of Information Technology.

Peter Okumah
Director of Information Technology
June 28, 2007