

North Central Charter Essential School

2006-2007 Student Acceptable Use Policy

Please read the following policy carefully and retain it for future reference. Once the student and student's parent(s) or guardian(s) have read this policy please sign and return the attached consent form. No users will be granted access to the NCCES network without a signed consent form for each year of attendance.

1. Purpose

North Central Charter Essential School (NCCES) is pleased to offer its users email accounts and access to the school's computer network, including access to the Internet. Access to these resources will enable users to explore thousands of libraries, databases, and other information resources.

NCCES believes that there can be tremendous educational value in the Internet, and recognizes the potential support to our curriculum. Because of its enormous size and resources, the Internet's educational potential is boundless. Because of its broad reach, however, the Internet also contains the potential for misuse. These guidelines are intended to help ensure the use this valuable resource in a safe and appropriate manner.

Families should be aware that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, or offensive. NCCES complies with the Federal Child Internet Protection Act (CIPA) by implementing content filtering services and by implementing this Student Acceptable Use Policy. While our goal is to provide Internet access to promote educationally supportive materials and sites, users will have access to other information as well. We believe that the benefits of user access to the Internet far exceed any disadvantages. NCCES makes every effort to ensure appropriate use of the Internet. Network users are expected to conduct themselves responsibly.

All use of the Internet is to be conducted under faculty supervision. Nevertheless, faculty members cannot monitor student use at every moment. Every user shall bear individual responsibility for his or her own appropriate use of the Internet.

The intent of this policy is to ensure that all uses of the network are consistent with NCCES educational goals.

2. Terms and Definitions

a. **NCCES Network (the network)** refers to the North Central Charter Essential School network and all associated resources. This includes, but is not limited to: computers and peripherals, network infrastructure, operating systems, software applications, domain structures, user accounts, e-mail, and Internet access.

b. **User** refers to any student or staff member with an NCCES account or anyone else provided access to resources associated with the our network.

c. This policy applies to all NCCES network users, and to the use of the our network and all associated resources whether or not they are connected to the network or physically on school property, and any device that is not the property of the North Central Charter Essential School but is used to connect to our network or any of its resources.

3. Network Access is a Privilege

a. Network access through NCCES resources is a privilege, not a right. A user's access may be canceled by school officials if this privilege is misused. Inappropriate conduct will be subject to disciplinary action, as outlined in this policy and in the NCCES Student Handbook.

4. Prohibited Activities

The North Central Charter Essential School (NCCES) considers the following uses of NCCES computers, the NCCES network, the Internet and other NCCES technology resources as unacceptable, and just cause for taking disciplinary action, revoking privileges, and/or initiating legal action:

4.1. Personal Safety

a. Users shall not post personal contact information about themselves or other people. Personal contact information includes **full name, address, telephone, school address, work address, etc.**

b. Users shall not agree to meet with someone they have met online without their parents' approval and participation.

c. Users shall promptly disclose to their teacher and or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

4.2. Illegal Activities

a. Users shall not attempt to gain unauthorized access to local or remote networks or computers, or go beyond their authorized access. This includes attempting to **log in to another person's account or access another person's files**. These actions are illegal, even if only for the purpose of browsing.

b. Users shall not make deliberate attempts to disrupt the computer system performance or destroy data by spreading computer viruses or by any other means. These actions are illegal.

c. Users will not use the system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of another person, etc.

d. Users shall not use NCCES computing resources for commercial or financial gain or fraud.

e. Users shall not use the network for political lobbying. Users may use the network to communicate with their elected representatives and to express their opinion on political issues.

f. Users shall not distribute bulk **unsolicited email messages (SPAM), chain letters or anonymous messages**.

4.3. Educational purposes

a. Users are granted access to the network for educational purposes only.

b. Users shall not participate in **chats, chatrooms, IM or computer games** unless approved, directed, and supervised by an appropriate member of the school faculty or administration.

c. Users shall not participate in "community" sites such as, but not limited to, **MySpace.com, FaceBook.com, Friendster.com** while using the NCCES network. Sites of this sort are not in support of the NCCES educational mission and they can be dangerous places for individuals.

4.4. System Security

- a. Users shall be responsible for the use of their individual account and shall take all reasonable precautions to prevent others from being able to use their account. **Under no conditions shall a user provide their account information and/or password to another person.**
- b. Users shall not **download, use, store or attempt to install any commercial, shareware or freeware software** without the express permission of the NCCES Technology Director.
- c. Users shall not intentionally circumvent security or filtering resources. Users will not access filtered sites by using **proxy sites or other methods of circumvention.**
- d. Users shall not change or attempt to change the configuration of any computers or network resources. This includes activities such as moving equipment, disconnecting equipment or changing equipment settings. Any changes must be approved by the NCCES Technology Director.
- e. Users shall immediately notify a teacher if they suspect or have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access
- f. Users shall avoid the inadvertent spreading of computer viruses.

4.5. Inappropriate Language

Restrictions against Inappropriate Language apply to public messages, private messages and material posted on Web pages. For the purpose of this policy, Inappropriate Language can be considered to include, not necessarily limited to, the following clarifications:

- a. Users shall not use obscene, profane, lewd, vulgar, rude, inflammatory, racist, sexist, threatening, or disrespectful language.
- b. Users shall not post information that, if acted upon, could cause damage or a danger of disruption.
- c. Users shall not engage in personal attacks, including prejudicial or discriminatory attacks.
- d. Users shall not harass another person. Harassment is persistently acting in manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, the user must stop sending messages to that person.
- e. Users shall not knowingly or recklessly post false or defamatory information about person or organization.

4.6. Respect for Privacy

- a. Users shall not repost a message that was sent to them privately without permission of the person who sent them the message.
- b. Users shall not post private information about another person.

4.7. Resource Availability

- a. Every effort shall be taken not to overuse finite resources. Users shall not download large files (over 1MB) unless absolutely necessary. If necessary, users shall download such files at a time when the system is not being heavily used and immediately remove the files from the system computer to their personal computer.
- b. Users shall not engage in any activity that affects the function of the network for other members of the NCCES community.

4.8. Plagiarism and Copyright Infringement

- a. Users shall not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings or others and presenting them as if they were original to the user.
- b. Users shall respect the rights of copyright owners. Users shall not download or distribute copyright-protected files. If the user is unsure whether they can use a work, they should request permission from the author or copyright owner. This applies to nearly all **music or video files that are not owned by the user including, but not limited to, MP3, WMA, WMV, AVI and MPG files**).

4.9. Access to Inappropriate Material

- a. For the purpose of this policy, Inappropriate Materials are those materials including, but not limited to, any materials not in support of the system's curriculum.
- b. Users shall not use the network to access material that is profane, pornographic or obscene, that advocates illegal acts, or that advocates violence or discrimination towards other people.
- c. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access to the computer teacher at their school. This will protect users against an allegation they have intentionally violated the Acceptable Use Policy.

5. Consequences of Violations

- a. In cases where it has been determined that a user has acted inappropriately, and depending on the extent and nature of the infraction and with consideration of the user's previous behavior, the appropriate administrative staff in consultation with the Director of Technology may take the following actions against the user:
 - Restricted network access.
 - Temporary or permanent loss of user account and privileges to access the network and all associated resources.
 - Disciplinary action up to and including suspension and expulsion.
 - Legal action, including criminal prosecution, as appropriate under local, state, and federal law.

6. Privacy and Monitoring

- a. Users should not assume that their use of the NCCES network will be private.
- b. All user files, including e-mail files and other Internet files and usage may be monitored by faculty for educational and administrative purposes, including the need to ensure the integrity of the network and the safety of our community.
- c. NCCES reserves the right to access and monitor all messages and information on the system, as it deems necessary and appropriate in the ordinary course of business, to prevent network abuse, to ensure the proper use of resources, and to conduct routine maintenance.
- d. Where appropriate, information may be disclosed to law enforcement officials in response to proper requests, or to other third parties in the context of proper requests in the course of litigation, without the prior consent of the information's creator, owner, sender or receiver.
- f. The NCCES network backup system automatically stores files and messages, including those that users "delete."

North Central Charter Essential School

2006-2007 Student Acceptable Use Policy

Consent Form

I have read the North Central Charter Essential School 2006-2007 Student Acceptable Use Policy and agree to use the technology resources in accordance thereof.

Further, my parent(s) or guardian(s) and I have been advised that the North Central Charter Essential School (NCCES) does not have control of the information on the Internet, which may contain material that is potentially offensive to some people. It is NCCES's intent to make network access available to further educational goals and objectives.

NCCES believes that the benefits to educators and students from access to the Internet, in the form of information resources and opportunities for collaboration, far exceed any disadvantages of access. Ultimately, however, the parent(s) or guardian(s) of minors are responsible for setting and conveying the standards that their child should follow. To that end, the North Central Charter Essential School supports and respects each family's right to decide whether or not to allow their child to utilize our network and the Internet.

The student and his/her parent(s) or guardian(s) shall understand that student access to the NCCES network is being provided in support of NCCES's educational program. The specific conditions and services being offered will change from time to time. In addition, NCCES makes no warranties with respect to the NCCES network, NCCES technology resources and the Internet, and it specifically assumes no responsibilities for:

- A. The content of any advice or information received by a user from a source outside NCCES, or any costs or charges incurred as a result of seeing or accepting such advice;
- B. Any costs, liability or damages caused by the way the user chooses to use his/her network access;
- C. Any consequences of service interruptions, data loss or corruption, or network changes even if these disruptions arise from circumstances under the control of NCCES.

WE HAVE READ AND DISCUSSED THIS POLICY AND AGREE TO ABIDE BY ITS PROVISIONS.

Student Name (please print): _____ Birthdate: _____

Signature of Parent/Guardian: _____ Date: : _____

IN ADDITION TO THE ABOVE SIGNATURES, PLEASE SIGN BELOW

I give my child permission to use the Internet for educational curricula reasons.

Signature of Parent/Guardian: _____ Date: : _____

Print Parent/Guardian Name: _____

Please return only this page – Keep all other pages for your future reference.