NORTH COW CREEK ELEMENTARY
Student Instructional Technology Acceptable Use and Internet Safety Policy

Technology provides a wealth of educational opportunities for staff and students. Access to these vast resources requires responsible use by each individual. It is important that you understand your rights and privileges when using the Western Placer Unified School District (NCCS) resources in this environment. This document describes the computer, network, and Internet resources made available by the school and your responsibilities and obligations in the use of these resources.

Introduction

NCCS is pleased to offer students access to district computers, communications systems[1], the Internet and an array of technology resources to promote educational excellence. Each student is responsible for their use of
technology, whether personal or district-provided. While using district and personal technology resources on or near school property, in school vehicles and at school-sponsored activities, as well as using district technology resources via off-campus remote access, each student must act in an appropriate manner consistent with school, district, and legal guidelines. It is the joint responsibility of school personnel and the parent or guardian of each student to educate the student about appropriate digital citizenship and to establish expectations when using technology.

District technology resources are provided to students to conduct research, complete assignments, and communicate with others in furthering their education. This focus does not allow the use of the network system for commercial, political, or personal entertainment purposes. Students may not offer, provide, or purchase products or services through the NCCS network system. The NCCS network system has not been established as a public access service or a public forum. Access is a privilege, not a right; as such, general rules of school behavior apply. Access to these services is given to students who agree to act in a considerate and responsible manner. Just as students are responsible for good behavior in a classroom or a school hallway, they must also be responsible when using school computer networks or personal technologies. Students must comply with school standards and honor this agreement to be permitted the use of technology. Disciplinary action may be taken against students for misuse of computer, network, and information resources.

[1](Communication systems include e-mail, web sites, blogging, podcasting, forums, wikis, and/or other emerging technologies).

Use of NCCES Network

- Each student, along with a respective parent/guardian, must sign an Acceptable Use Policy (AUP) Agreement to be granted an account on the NCCES network system.
- Students will not make deliberate attempts to disrupt or harm the computer system and its hardware or destroy data by spreading computer viruses or by any other means. Use or possession of "hacking" tools are prohibited.
- Students will use their personal server storage to store only files that are educational in nature and related to course work.
- Students are expected to maintain their instructional files and media in a responsible manner, which includes backing up files at regular intervals to a memory device and deleting files at the end of the school year.
- Students are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a student provide their password to another person except to a school administrator or parent.
- Students will not attempt to log on or connect to the NCCS network under any identity other than their own username.
- Students will not attempt to gain unauthorized access (including hacking) to the NCCS network system or to any other computer system through the NCCS network system or go beyond their authorized access. This includes attempting to log in through another person's account or access another person's files. These actions are inappropriate, even if only for the purposes of "browsing" and may result in disciplinary action.
- Students will immediately notify a teacher if they have identified a possible security problem.
- Students will use school resources (e.g. printers, cameras, etc.) only for educational purposes.
- Students are not permitted to connect any personal devices (e.g. laptops, smart phones, etc.) to any part of the NCCS network system (wireless or directly plugged) without first gaining approval from the Technology Department.
- Students will not download or upload programs or files that can be run or launched.
- Use of NCCS computers, network, and Internet services does not create any expectation of privacy.
- Students should expect routine monitoring of computer usage and Internet browsing while logged on to the NCCS network.
- Parents have the right to request to see the contents of student files.

Internet Access

- All students will have access to the Internet and World Wide Web information resources through computers connected to the network.
- NCCS actively uses filtering software hosted by the Placer County Office of Education to meet the Children's Internet Protection Act (CIPA) requirement and to prevent students from accessing graphics that are (1) obscene, (2) pornographic, or (3) harmful to minors. NCCS retains the right to block unacceptable web sites. Filtering software is not a perfect science and it may be possible for users to access inappropriate sites.
- NCCS does not guarantee network functionality or accuracy of information.
- Students will not use the NCCS network system to access inappropriate material including sites that display profane or obscene (pornography) material, advocates illegal acts, encourages the use of drugs, alcohol or tobacco, school cheating, weapons, material that advocates violence, participation in hate groups, or discrimination towards other people, or other inappropriate activities considered harmful to minors.
- If students mistakenly access inappropriate information, they should immediately minimize their screen and tell their teacher. This will protect the student against a claim that they have intentionally violated this Policy.
- The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.

Use of Messaging Services[2]

- A filtered E-mail account may be provided to students for educational purposes and not as a public or student forum.
- Students will promptly disclose to their teacher or other school employee any message or information they receive that is inappropriate or makes them feel uncomfortable while on the web, using e-mail, chat rooms, forums or other forms of messaging services.
- E-mail, if provided, may not be used for unlawful activities, political or commercial purposes, any form of harassment or threats, sending of spam messages or chain letters to more than five people or any use that interferes with the school computing services or its employees.
- Students may not send messages with a false identity or alter forwarded mail out of context.
- Students will abide by rules of Network etiquette by not using defamatory, inaccurate, abusive, obscene, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or prejudicial language in public or private communication.
- Students will not post personal contact information about themselves or other people without parental approval. Personal contact information includes but not limited to names, home, school, parent work addresses, telephone numbers, personal photos or videos.
- Students will not repost a message that was sent to them privately without permission of the person who sent them the message.
- Students will not post or share information that could cause damage or a danger of disruption to
- NCCS schools or any other organization or person.
- Students are prohibited from accessing or attempting to access instant messages, chat rooms, forums, e-mail, social networking sites, or other messaging services during the instructional day unless authorized by a teacher or administrator for instructional purposes.

[2] (e-mail, chat, forums, blogs, social networking, instant message, SMS and other forms of messaging services)

Web Applications[3]

Students' use of digital media and environments to communicate and work collaboratively to support individual learning and contribute to the learning of others is a key performance indicator of 21st Century Skills. Students may interact, collaborate, and publish with peers, experts, or others employing a variety of digital environments and media. In a digital environment, students will follow all established Internet safety guidelines including the following conditions:

- The use of digital media is considered an extension of your classroom. Any speech that is considered inappropriate in the classroom is also inappropriate in all digital environments. This includes but is not limited to profanity; racist, sexist or discriminatory remarks.
- Students using digital media are expected to act safely by keeping ALL personal information out of their posts.
- A student should NEVER post personal information on the web (including, but not limited to, last names, personal details including address or phone numbers, or photographs). Do not, under any circumstances, agree to meet someone you have met over the Internet.
- Never link to web sites from your digital environment without reading the entire article to ensure it is appropriate for a school setting.
- Students using such tools agree to not share their user name or password with anyone besides their teachers and

parents and treat digital spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate online.
- Students who do not abide by these terms and conditions may lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse according to the school discipline policy.

[3] (e-mail, chat, forums, blogs, social networking, instant message, wikis, and other forms of collaborative software)

Cyberbullying
- NCCS expressly forbids cyberbullying. For the purposes of this policy, "cyberbullying" shall mean using messaging services[2] and/or other digital communication devices to bully others by:
- Sending or posting cruel messages or images;
- Threatening others;
- Excluding or attempting to exclude others from activities or organizations;
- Starting or passing on rumors about others or the school system;
- Harassing or intimidating others;
- Sending angry, rude or vulgar messages directed at a person or persons privately or to an online group;
- Sending or posting harmful, untrue or cruel statements about a person to others;
- Pretending to be someone else and sending or posting material that makes that person look bad or places that person in potential danger;
- Sending or posting material about a person that contains sensitive, private or embarrassing information, including forwarding private messages or images;
- Engaging in tricks to solicit embarrassing information that is then made public.
- Using camera and/or video enabled devices to bully another person or to invade another person's privacy.

Privacy, Plagiarism, Piracy and Copyright Infringement
- An image taken by any camera or video enabled device may not be published, broadcast, or transmitted to any other person, by any means, without the knowledge and consent of each person appearing in that image who had a reasonable expectation of privacy at the time the image was recorded or the person who owns the copyright in the material appearing in that image.
- Camera and/or video enabled devices may not be used in any classroom without a teacher's written permission.
- Students will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were yours. Plagiarism could result in loss of grade for the assignment in addition to other consequences.
- Students will not download or install pirated software, music, video or files that infringe on copyright laws onto computers. Possession of unlicensed or pirated software is illegal.
- Students will respect the rights of copyright owners. Copyright infringement occurs when you inappropriately reproduce a work that is protected by a copyright. If a work contains language that specifies appropriate use of that work, you should follow the expressed requirements.
- If you are unsure whether or not you can use a work, you should request permission from the copyright owner. Copyright law can be very confusing. If you have questions ask a teacher.

Use of School Hardware[4]
- School hardware will not be left unattended.
- In the event of any damage to school hardware at any time while it is in the student's possession, the student agrees to inform the appropriate NCCS Technology Service Center so that repairs can be performed.

[4](Hardware systems include laptops, digital camera/video equipment and/or other technologies).

Consequences
- In the event there is a claim that a student has violated this policy in the use of the NCCS network system, the student will be provided with a written notice of the suspected violation and an opportunity to present an explanation before an administrator.
- If a student is found to have violated this Policy, the consequences will be, but not limited to, warnings, usage restrictions being placed on their network account, or disciplinary action at the discretion of the site administration.
- A violation of Federal, State or local laws or ordinances may result in legal proceedings.

NORTH COW CREEK ELEMENTARY SCHOOL DISTRICT
Instructional Technology Acceptable Use and Internet Safety Policy Agreement

I understand and will abide by the Acceptable Use and Internet Safety Policy. Should I commit a violation, I understand that consequences of my actions could include suspension of computer privileges, school disciplinary action, and/or referral to law enforcement.

Student's Name (please print): _____

Student's Signature:_____Date _____

Parent or Guardian:

As the parent or guardian of this student, I have read the Acceptable Conduct and Use Agreement. I understand that computer access is provided for educational purposes in keeping with the academic goals of the North Cow Creek School District (NCCS), and that student use for any other purpose is inappropriate. I recognize it is impossible for NCCS to restrict access to all controversial materials and I agree to not hold the district or any district staff responsible for the failure of any technology protection measures, violations of copyright restrictions, or users' mistakes or negligence. I hereby give permission for my child to use computer resources at NCCS, including web or Internet based services provided by other companies or institutions which have been approved by NCCS for student use.

I hereby give permission for my child to use computer resources at NCCS.

Parent or Guardian's Name (please print) _____

Parent or Guardian's Signature_____Date _____