Student Responsible Use Agreement for Use of internet, Computer Equipment, and other Technology at Northern Wells Community Schools

Introduction

Northern Wells Community Schools (NWCS) recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop progressive technology and communication skills.

NWCS is committed to providing educational opportunities for all students and maintains compliance with the Individuals with Disabilities Education Act 2004 (20 U.S.C. 1400 et seq.).

To that end, we provide the privilege of access to technologies for student and staff use.

This Responsible Use Policy outlines the guidelines and behaviors that all users are expected to follow when using school technologies or when using personally---owned devices on the school campus.

- The Northern Wells Community Schools network is intended for educational purposes.
- All activity over the network or using district technologies may be monitored, documented and retained.
- Access to online content via the network may be restricted in accordance with our policies and federal regulations, such as the Children's internet Protection Act (CIPA).
- Students are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources may result in disciplinary action.
- Using an internet filter and other technologies, Northern Wells Community Schools makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Technologies Covered

NWCS may provide the privilege of internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

This Responsible Use Policy applies to both school—owned technology equipment utilizing the NWCS network, the NWCS internet connection, and/or private networks/internet connections accessed from school—owned devices at any time. This Responsible Use Policy also applies to privately—owned devices accessing the NWCS network, the NWCS internet connection, and/or private networks/internet connections while on school property. As relevant new

technologies emerge, NWCS will seek to provide access to them. The policies outlined in this document cover *all* available technologies now and in the future, not just those specifically listed or currently available.

Usage Policies

All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics as well as the spirit of this document. Users should be safe, appropriate, careful and kind; not try to get around technological protection measures; use good common sense; and ask if they don't know.

Web Access

NWCS provides its users the privilege of access to the internet, including web sites, resources, content, and online tools. Access to the internet will be restricted as required to comply with CIPA regulations and school policies. Web browsing may be monitored, and web activity records may be retained indefinitely.

Users are expected to respect the web filter as a safety precaution, and shall not attempt to circumvent the web filter when browsing the internet. The determination of whether material is appropriate or inappropriate is based solely on the content of the material and the intended use of the material, not on whether a website has been blocked or not. If a user believes a site is unnecessarily blocked, the user should submit a request for website review through the teacher, who may contact his/her building principal.

Email

NWCS may provide users with the privilege of email accounts for the purpose of school—related communication. Availability and use may be restricted based on school policies.

If users are provided with email accounts, the account(s) should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origins; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Social/Web 2.0 / Collaborative Content

Recognizing the benefits collaboration brings to education, NWCS may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally identifying information online.

Student Social Media Policy

Social media shall be defined as internet-based applications that turn communication into interactive dialogue between users. These policies are established for the protection of everyone involved.

Online behavior should reflect the same standards of honesty, respect, and consideration that is used face to face.

A. Students should be aware of what they post online. Social media venues, including wikis, blogs, photo and video sharing sites, etc. are very public. Students should not post anything they wouldn't want others to see.

B. Students should follow the school's handbook guidelines when writing online. It is acceptable to disagree with someone else's opinions; however, it should be done in a respectful way. What is inappropriate in the classroom is inappropriate online.

C. Students should never give out personal information, including but not limited to last names, phone numbers, addresses, birthdates, and pictures. Students should not share their passwords with anyone besides teachers and parents.

D. Students should do their own work. Students should not use other people's intellectual property without that person's permission. It is a violation of copyright law to copy and paste others' thoughts without giving credit. When paraphrasing another's ideas students should cite sources accurately. Pictures may also be protected under copyright. Students should have permission to use the image or should verify that it is under Creative Commons attribution.

E. Students should not use any device to capture, record, or transmit the words (audio) and or images (pictures or video) of any student, staff member, or other person in the school, in locker rooms or bathrooms.

F. Students should not use social media sites to post comments, photos, or videos with the intent of scaring, embarrassing, hurting, bullying, or intimidating someone else.

Mobile Devices Policy

NWCS may provide users with mobile computers or other devices to promote learning outside of the classroom. Users should abide by the same Responsible Use Policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to users care. Users should immediately report any loss, damage, or malfunction to IT staff. Users may be financially accountable for any damage resulting from negligence or misuse.

Use of school—issued mobile devices off the school network may be monitored.

Personally Owned Devices Policy

In some cases, a separate network may be provided for personally owned devices. Please remember, this Responsible Use Policy applies to privately owned devices accessing the NWCS network, the NWCS internet connection, and private networks/internet connections while on school property.

Security

Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. Users should never share personal information.

If users believe a computer or mobile device they are using might be infected with a virus, they should alert IT. Users should not attempt to remove the virus themselves or download any programs to help remove the virus.

Downloads

Users should not download or attempt to download or run programs over the school network or onto school resources without express permission from IT staff.

Users may be able to download other file types, such as images, videos, files, and apps. For the security of the network users should download such files only from reputable sites, and only for education purposes. It is important, however, to remember that devices have limited storage capacities. It will be important for users to manage storage with the understanding that all school-related apps and files take precedent over others.

Netiquette

Users should always use the internet, network resources, and online sites in a courteous and respectful manner.

Users should recognize that among the valuable content online there is also unverified, incorrect, or inappropriate content. Users should only use trusted sources when conducting research via the internet.

Users should remember not to post anything online that they wouldn't want students, parents, teachers, or future colleges or employers to see. Once something is online, it cannot be completely retracted and can sometimes be shared and spread in ways the user never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words, music, or images, from the internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Information obtained via the internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the internet without adult permission. Users should recognize that communicating over the internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet in real life someone they meet online without parental permission.

If users see a message, comment, image, or anything else online that makes them concerned for their personal safety, they should immediately bring it to the attention of an adult (teacher or staff if at school; parent if using the device at home).

Cyberbullying

Cyberbullying will not be tolerated. Harassing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Users should not be mean or send emails or post comments with the intent of scaring, hurting, embarrassing or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges. In some cases, cyberbullying can be a crime. Remember that online activities may be monitored and retained.

All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

Examples of Responsible Use

I will:

- Use school technologies for school—related activities.
- Bring my device to school fully charged and in its protective case.
- Keep private information private. My password and identity are mine and not to be shared with anyone other than my parent / guardian.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places, for educational purposes.
- Cite sources when using online sites and resources for research.
- Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of others and myself.
- Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Irresponsible Use

I will **not**:

- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images or content.
- Engage in cyberbullying, harassment, or disrespectful conduct toward others.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post personally identifying information, about others or myself.
- Agree to meet in person someone I meet online.
- Use language online that would be inappropriate in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, or content that isn't intended for my use.
- Use other students' online accounts.
- Take inappropriate pictures and / or record inappropriate audio/video of other people. The school staff or subjects of such pictures, audio, or video will determine the appropriateness of these actions.
- Pretend to be anyone other than myself when online or creating accounts.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

NWCS will not be responsible for damage or harm to persons, files, data, or hardware.

While NWCS employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

NWCS will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of this Responsible Use Policy

Violations of this policy may have disciplinary consequences, including:

- Suspension of network, technology, or computer privileges;
- Notification of parents;
- Detention, suspension, or expulsion from school and school---related activities;
- Legal action and/or prosecution.

Staff, Students and Parents/Guardians shall be required to sign Northern Wells Community Schools' Responsible Use Agreement annually before Internet or network access shall be allowed.

Student Name:_____

Student Signature:_____Date:_____

If student is under eighteen (18) years of age, parent/guardian signature is required.

Parent/Guardian:_____ Date:_____

Updated: 6/5/2014