Wa-Nee Community Schools

Good Digital Citizenship: Responsible Use Agreement for Students

Leading Education And Progress

Merging the Past, Present, and Future of Learning

Good Digital Citizenship: Responsible Use Agreement for Students

1. Introduction

This Responsible Use Agreement (RUA) outlines the guidelines and behaviors that users are expected to follow when using school technologies. This agreement along with the Acceptable Use Agreement are policies that should be followed anytime that district technologies are being used.

a. Wa-Nee Community Schools (WCS) technology and networks are intended for educational purposes only.
b. All activity over the network or while using the district technologies will be monitored and retained.
c. Access to online content via the WCS network will be filtered in accordance with our policies and federal regulations, including the Children's Internet Protection Act (CIPA).
d. Users are expected to follow the same rules for good behavior and respectful conduct online as offline.
e. Misuse of school resources can result in disciplinary action.
f. WCS makes a reasonable effort to ensure users' safety and security online, but will not be held accountable for any harm or damages that result from the use of school technologies.
g. Users of the district network or other technologies are expected to immediately alert district personnel of any concerns for safety or security.

2. Technologies Covered

WCS may provide the privilege of Internet access, computers, mobile devices, video conferencing capabilities, collaboration capabilities, message boards, email and more. As new technologies emerge, WCS will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed or currently available.

This Responsible Use Policy applies to both school-owned technology equipment utilizing the WCS network or other internet connections accessed from school-owned devices at any time. This Responsible Use Policy also applies to privately-owned devices accessing the WCS network while on school property.

3. Usage Policies

All technologies provided by the district are intended for educational purposes. All users are expected to use good judgement and to follow the specifics of this document 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 have questions.

a. Users should follow the same responsible use policies when using school devices off the school network as on the school network.
b. Users are expected to treat all school devices with extreme care and caution.
c. Users should report any lost/stolen, damaged, or malfunctioning devices to school personnel immediately.
d. Users will be financially accountable for any damage resulting from negligence or misuse.

4. Web Access

WCS 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 whether a website has been blocked or not. If a user believes a site is unnecessarily blocked or should be blocked and is not, the user should submit a request for website review through the teacher, who will then contact technology personnel.

5. Email

WCS will provide users with the privilege of email accounts for the purpose of school-related communication. Email accounts are hosted on Microsoft's servers (Office 365) and availability and use is restricted based on school policies.

If users are provided with email accounts the account should be used with care. Users should not send personal information or attempt to open files or follow links from unknown or untrusted origins. Users should use appropriate language and 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 is monitored and archived.

6. Social and Collaborative Content
Recognizing the benefits collaboration brings to education, WCS will provide users with access to websites or tools – that will include Microsoft Office 365 (O365). These tools will allow for 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.

7. Mobile Devices Policy
WCS 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 user's care. Users should immediately report any loss, damage, or malfunction to building technology personnel.

8. 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 WCS network, the WCS internet connection, and private networks/internet connections while on school property.

9. Security
Users are expected to take reasonable safeguards against 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 building technology personnel. Users should not attempt to remove the virus themselves or download any programs to help remove the virus.

10. Downloads
Users should not attempt to download or install programs via the school network or onto school resources unless approved by the Technology Department. All approved software will either be installed by the Technology Department or made available in Software Center for user installation.

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

11. 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 always 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.

12. 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 did not create themselves, or misrepresent themselves as an author or creator of something found online. Information obtained via the internet should be appropriately cited, giving full credit to the original author.

13. Personal Safety

Users should never share personal information including phone number, address, social security number, birthday, or financial information over the internet without permission from an adult. Users 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.

14. Cyberbullying

Cyberbullying will not be tolerated and can take on many forms. Understanding the different ways technology can be used to hurt others can help prevent it from happening.

a. **Flaming**- Online fights using electronic messages with angry or vulgar language.
b. **Harassment**- Repeatedly sending nasty, mean, and insulting messages.
c. **Denigration**- "Dissing" someone online. Sending or posting gossip or rumors about a person to damage his or her reputation or friendships.
d. **Impersonation**- Pretending to be someone else and sending or posting material to get that person in trouble or damage their reputation.
e. **Outing**- Sharing someone's secrets or embarrassing information or images online.
f. **Trickery-** Tricking someone into revealing secrets or embarrassing information and then sharing it online.
g. **Exclusion-** Intentionally and cruelly excluding someone.
h. **Cyberstalking**- Repeated, intense harassment and denigration that includes threats or creates significant fear.

**From "An Educator's Guide to Cyberbullying and Cyber-Threats," by Nancy Willard*

15. WCS Position on Cyber Bullying and Digital Citizenship

a. Cyberbullying will not be tolerated and is strictly forbidden.
b. Engaging in cyberbullying to harm (physically or emotionally) another person will result in severe disciplinary action and loss of privileges.
c. In some cases, cyberbullying can be a crime.
d. Users should remember that digital activities are monitored and retained.
e. Students shall receive age-appropriate education including, but not limited to appropriate online behaviors in social networking sites, chat rooms, electronic communications etc.; the dangers inherent with the online disclosure of personally identifiable information; and, consequences of unlawful activities, including cyberbullying awareness and response, and other unlawful or inappropriate online activities by students.

16. Limitation of Liability

WCS will not be responsible for damage or harm to persons, files, data, or hardware. While WCS employs filtering and other safety and security measures, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness.

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

17. 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.

Examples of Responsible Use of School Technologies

- Use school technologies at appropriate times, in approved places, for educational purposes.
- Bring the device to school fully charged and in its protective case if applicable.
- Keep private information private. My username and password are not to be shared with anyone other than a 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 the operation of equipment.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or staff member if I see threatening, inappropriate, or harmful content (images, messages, and posts) online.
- Cite sources when using online sites and resources for research.
- Recognize that using 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 judgement when using school technologies.

Examples of Irresponsible Use of School Technologies

- Use school technologies in a way that could be personally or physically harmful.
- Attempt to find inappropriate images and content.
- Share private information that should be kept private. Your username and password are not to be shared with anyone other than a parent/guardian.
- 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 found online.

- Post personally identifying information.
- Agree to meet in person someone met 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 student use.
- Use other students' online accounts.
- Taking inappropriate pictures and/or recording inappropriate audio/video of other people.
- Pretend to be someone else when online or creating accounts.

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

Students and Parents/Guardians shall be required to sign the Wa-Nee Community Schools' Responsible Use Agreement annually before internet or network access shall be allowed.

Responsible Use Agreement for Students

Your signature indicates that you have read and agree to all polices and guidelines contained in the *Acceptable Use* and *Responsible Use Agreement* documents.

Student Name: _____

Student Signature: _____ Date: _____

Parent/Guardian Signature: _____ Date: _____