The purpose of the White Salmon Valley School District Responsible Use Policy (RUP) is to provide guidelines, rules, and the code of conduct for the use of electronic devices, technology resources and the WSVSD network. The WSVSD School Board of Directors recognizes that information posted on the Internet is public and permanent and can have a long-term impact. These procedures are written to support policies 3245 & 2022 and to promote positive and effective digital citizenship among students. Expectations for student behavior online are no different from face-to-face interactions.

Users of the district’s electronic resources need to read, understand, and abide by the policies spelled out in this Responsible User Agreement. It outlines the guidelines and behaviors users are expected to follow when using school technologies. All users are expected to use good judgment and to follow the specifics of this document.

- The network is intended for educational purposes
- All activity over the network or using district technologies may be monitored and retained
- Access to online content via the network will 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 can result in disciplinary action. Law enforcement will be consulted when necessary
- We make a reasonable effort to ensure students’ safety and security online, but will not be held accountable for any harm or damages that result from misuse of technologies in school.
- Users of the network or other technologies are expected to alert the Technology Department immediately of any concerns for safety or security

Technologies Covered
WSVSD may provide Internet access, desktop computers, laptops, tablets, video conferencing, online collaboration and more. The district reserves the right to prioritize the use of, and access to, the network. All use of the network must support education and be consistent with the mission of the district. As new technologies emerge, WSVSD 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.

Web Access & Filtering/Monitoring
WSVSD provides its users with access to the Internet, including web sites, resources, content, and online tools. The district reserves the right to monitor, inspect, copy, review and store without prior notice information about the content and usage of:

- User applications and bandwidth utilization
- User document files, folders and electronic communications
- Web/Internet access
- Any and all information transmitted or received in connection with the network

No student should have any expectation of privacy when using the district’s network. The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Access will be restricted in compliance with the Children’s Internet Protection Act (CIPA) regulations and school policies. Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the CIPA, and other objectionable material may also be filtered. The determination of what constitutes “other objectionable” material is a local decision. Users should keep in mind:

- Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the district’s Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to district browser settings and any
other techniques designed to evade filtering or enable the publication of inappropriate content);

- E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
- The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district devices;

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn’t be, the user should follow protocol to alert an IT staff member or submit the site for review.

To comply with requirements under CIPA, 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. Age appropriate materials will be made available for use across grade levels. Training on online safety issues and materials for implementation will be made available to administration, staff and families.

Email
The WSVSD may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies and a student’s age or grade. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher.

Email usage may be monitored and archived.

- Students 7-10 with parent approval will be issued a whitesalmonschools.org student account that can only send and receive email with other users within the whitesalmonschools.org domain.
- Students 11-12 with parent approval will be issued a whitesalmonschools.org account with the ability to email outside of the whitesalmonschools.org domain. This will allow students to communicate/collaborate with peer mentors, colleges and apply for scholarships.

Backups are made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outages or intermittent technical issues, staff and student files are backed up on district servers regularly. Refer to the district retention policy for specific records retention requirements.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline.

Social / Collaborative Content
Recognizing that collaboration is essential to education, WSVSD may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users. Posts, chats, sharing, and messaging may be monitored.

Mobile Devices Policy
School-Issued Devices
WSVSD may provide users with electronic devices (e.g. ipads, chromebooks, tablets) to promote learning both inside and outside 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 your care. Users should report any loss, damage, or malfunction to IT staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.

Personally-Owned Devices
In accordance with district policies and procedures, (policy 3245) students may use their own personal electronic devices in a manner that does not pose a threat to academic integrity, disrupts the learning environment or violates the privacy of others. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day. Use of personally owned devices on the school network may be monitored and subject to the policies on this
agreement. Students are responsible for devices they bring to school or school sponsored events. The district shall not be responsible for loss, theft or destruction of devices brought onto school property.

**Security**

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Students are responsible for all activity on their account and must not share their account password. The following procedures are designed to safeguard network user accounts:

- All users must be positively identified, by using a user ID and password, prior to being able to use any network or information resource.
- Change passwords according to district policy;
- Users are prohibited from using a user ID that is assigned to another user
- Users must log off or lock their computer when leaving it unattended for any period of time
- Users are prohibited from using an anonymous or guest user account
- Do not insert passwords into e-mail or other communications;
- If you write down your user account password, keep it in a secure location;
- Do not store passwords in a file without encryption;
- Do not use the “remember password” feature of Internet browsers

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. If you believe a computer or mobile device you are using might be infected with a virus, please alert IT staff. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

**Downloads**

Users should not download, attempt to download, or run executable programs over the school network or onto school resources without express permission from IT staff. You may be able to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites, and only for educational purposes.

**Netiquette**

Netiquette is a term that describes proper online behavior.

- Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.
- Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research.
- Users should also remember not to post anything online that they wouldn’t want parents, teachers, or future colleges or employers to see. Once something is online, it’s out there—and can sometimes be shared and spread in ways you never intended.

**Ownership of Work**

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. Staff members must obtain a student’s permission prior to distributing his/her work to parties outside WSVSD.

**Personal Safety**

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

- Users should never share personal information about themselves or another individual, 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.
White Salmon Valley School District Responsible User Agreement

- Users should never agree to meet someone they meet online in real life without parental permission.
- Users may not post student pictures or names on any public class, school or district website unless the appropriate permission has been obtained according to district policy; and
- If users encounter dangerous or inappropriate information or messages, they should notify the appropriate school authorities immediately.

Bullying
Bullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don’t be mean. Don’t send emails or post comments with the intent of scaring, hurting, 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 your activities are monitored and retained.

Limitation of Liability
The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries or service interruptions caused by his/her own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district’s computer network or the Internet.

Violations of this Responsible Use Policy
Violation of any of the conditions of use explained in the White Salmon Valley School District’s Electronic Resources policy 2022 or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.
Examples of Responsible Use
I will:

● Use school technologies for school-related activities and research.
● 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/bullying, inappropriate, or harmful content (images, messages, posts) online.
● Use school technologies at appropriate times, in approved places, for educational pursuits only.
● Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
● Recognize that use of school technologies is a privilege and treat it as such.
● Be cautious to protect the safety of myself and others.
● 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 to myself or others.
● Search inappropriate images or content.
● Engage in cyberbullying, harassment, or disrespectful conduct toward others—staff or students.
● Try to find ways to circumvent the school’s safety measures and filtering tools.
● Use school technologies to send spam or chain mail.
● Post personally-identifying information, about myself or others, or agree to meet someone I met online.
● Use language online that would be unacceptable in the classroom.
● Use school technologies for illegal activities or to pursue information on such activities.
● Attempt to hack, crack, vandalize or access sites, servers, accounts, or content that isn’t intended for my use.
● Support or oppose ballot measures, candidates and any other political activity, except as an educational / learning activity (e.g., persuasive writing, civics assignment, etc.);
● Attach unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken.

I have read and understood this Responsible Use Policy and agree to abide by it:

__________________________________________
(Student Printed Name)

__________________________________________
(Student Signature)

__________________________________________
(Grade)                                (Date)

I have read and discussed this Responsible Use Policy with my child:

__________________________________________
(Parent Printed Name)

__________________________________________
(Parent Signature)

__________________________________________
(Date)

Publishing Information on the WSVSD Websites & School Email

Yes  No  Please check each permission to allow publication of student work or information on the WSVSD websites.

I grant permission to publish the first and last name of the student named above on WSVSD web pages.

I grant permission to publish identifiable photographs of the student named above on the WSVSD websites.

I grant permission to issue the student named above a school email account for educational use while enrolled at WSVSD. Student email accounts are within a protected domain; students can only email with other users within the whitesalmonschools.org domain.

**District Use Only:** Permissions logged ☐ Google account created ☐ Grad Year _____ Date ______ Initials _____