ELECTRONIC RESOURCES AND INTERNET SAFETY

The Sumner-Bonney Lake School District views the use of electronic resources as central to the delivery of its educational program and expects that all students and staff will use electronic resources as an essential part of learning, working, and interacting with the community. The Sumner-Bonney Lake School District strives to maintain an environment that promotes ethical and responsible conduct in all electronic resource activities by staff and students. These procedures are written to supplement Sumner-Bonney Lake School District Policy 2022 Electronic Resources and to promote the appropriate and responsible use of technology in furthering the District's mission and Board of Directors' goals. Furthermore, the District does employ filtering software on all mobile devices to maintain compliance with FCC regulations related to Children's Internet Protection Act (CIPA), Children's Online Privacy Protection Act (COPPA) and the e-rate program administered by Universal Service Administration Company (USAC.) Any employee, student, or other individual engaged in activity that involves the District's electronic resources must comply with the established policy and procedures.

These procedures are delivered electronically to all end users and subject to revision and/or adaptation more easily based on our changing use of technology and end-user sophistication. End users will be prompted upon login to accept and agree that s/he will abide by Board Policy 2022 (Electronic Resources ***and Internet Safety****) and* ***Electronic Resources*** *Procedure 2022P. If, during the login process, an end user declines or disagrees with these procedures the system will disallow the end user's account and/or end user's device from accessing components of or complete access to Sumner-Bonney Lake School District resources. It is the school district's intent to provide access to end users that meet compliance without compromising on the educational value and efficiencies that accompany access. This process is outlined in the District's* ***Electronic Resources and Internet Safety*** *& Procedures available on the District Website. Hard copy records of this document can be obtained from a school or the district office.*

Parents have the option to Opt-Out or Decline access to all technology resources by using the Electronic Resources Form 2022F. This form is available via the School District's website. The decision to opt out of all technology resources does have a potential impact on daily instruction.

ELECTRONIC RIGHTS AND RESPONSIBILITIES

Sumner-Bonney Lake School District Responsibilities

The Sumner-Bonney Lake School District recognizes its obligation to both protect the well-being

of students in its charge and to be the steward of public property and resources. To these ends, the District reserves the right to, and may at any time, do the following:

- Log electronic resource use and monitor fileserver space utilization by users. The District assumes no responsibility or liability for files deleted due to violation of file server space.
- Monitor the use of activities through the District's networks and electronic resources. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity.
- Provide internal and external controls as appropriate, including the right to determine who will have access to Sumner-Bonney Lake School District-owned equipment.
- Restrict or exclude those who do not abide by the Sumner-Bonney Lake School District's electronic resources policy or other policies governing the use of school resources.
- Report to appropriate authorities apparent violations of the law discovered through the District's monitoring of electronic resources.
- Restrict electronic resource destinations through software or other means.
- Provide guidelines and make reasonable efforts to train staff and students in responsible use and policies governing electronic resource communications.
- Monitor and maintain mailing list subscriptions and delete files from the personal mail directories to avoid excessive use of file server hard-disk space.
- Use filtering software to block or filter access to visual depictions that are obscene and all child pornography in accordance with CIPA. Other objectionable material may likewise be filtered. The determination of what constitutes "objectionable" material is determined by the District's administration consistent with the District's educational mission, the District's policies and procedures, and the Board of Directors' goals.
- Implement and maintain appropriate data privacy and security measures for all electronic resources, including AI systems, to protect student and staff data in accordance with Policy 6501 - Data Privacy and procedure 6501P - Data Privacy Procedure

User Responsibilities
It is expected that staff and students will use electronic resources provided by the Sumner-Bonney Lake School District in work and study. However, the failure of a staff member, student, or any other person to comply with these procedures while using the District's electronic resources may result in restricted access up to and including a complete denial of access.

All use of the electronic resources must be consistent with the mission and objectives of the Sumner-Bonney Lake School District, further district goals established by the Board of Directors, and be in compliance with district policy and procedure.

District staff must at all times maintain the confidentiality of confidential student data in

accordance with the Family Educational Rights and Privacy Act (FERPA) and corresponding state law.

Those who use district-owned and maintained technologies, i.e., devices or electronic resources, to access the Internet at home are responsible for: inappropriate cached content; replacement or repair cost; and configuration of such use.

Staff Responsibilities
Staff members who supervise students, control electronic equipment, or otherwise have occasion to observe student use of said equipment shall make reasonable efforts to monitor the use of this equipment to assure that it conforms to electronic resources procedures and is consistent with the mission and goals of the Sumner-Bonney Lake School District. Staff should make reasonable efforts to become familiar with the electronic resources and their use so that effective monitoring, instruction, and assistance may be provided. Staff should report any misuse to their supervisor.

Responsible use by student, staff and guests shall include the following:

- Creation of files, projects, videos, Web pages, podcasts, and other activities using electronic resources, consistent with the educational mission of the District and in compliance with District polic**ies** and procedur**es**.
- Participation in electronic communication and collaboration activities such as blogs, wikis, podcasts, email, shared documents, and other activities using electronic resources, consistent with the educational mission of the District and in compliance with District polic**ies** and procedur**es**.
- Participation in district-sponsored social media to inform and communicate with members of the school district community consistent with the educational mission of the District and in compliance with polic**ies** and procedur**es**.
- With parent permission, posting of student-created original educational material, curriculum-related materials and student work. Sources outside the classroom or school must be appropriately cited and all copyright laws must be followed.
- Student and staff use of the network for incidental personal use shall be in accordance with all District policies and procedures. Such incidental work, while not prohibited, will not be provided any additional staffing resources to support or enable.
- Users will help maintain a safe computing environment by notifying a teacher or Technology Services when a security, filtering or inappropriate content is detected. Users must not demonstrate **the** problem to other users.

Unacceptable Use and Preventative Measures

- Users must respect the privacy of others. Unauthorized access or unauthorized disclosure of personal information of students, staff, or other individuals for whom the District retains records. "Personal information" includes education records or data, employment records, and personal addresses, phone numbers, or email addresses.
- Contributing to cyberbullying, chain letters, harassment, intimidation, denigrating comments, discriminatory remarks, and other similar conduct. Including but not limited to using or forwarding profanity, obscenity, vulgar language, racist terms, or other language that is offensive to a reasonable person. All users must comply with policies 3207, 5011, and 5012.
- Any use of electronic resources for individual profit or gain; for product advertisement; for political action or political activities; or for excessive personal use. "Political action or political activities" includes support of or opposition to political campaigns, candidates, ballot measures, or lobbying for or in opposition to legislation.
- Playing games, accessing social networking sites without specific authorization, and streaming or downloading audio and video files unless specifically authorized by a teacher for instructional purposes.
- Intentionally seeking information on, obtaining copies of, or modifying files, other data, or passwords belonging to other users, or misrepresenting other users on the electronic resources. The user may not send electronic communications fraudulently.
- Using an electronic account authorized for another person.
- Producing or making use of the electronic resources in a manner that serves to substantially disrupt the use of the network by others.
- Unauthorized downloading or installation, destroying, modifying, or abusing hardware and/or softwares, including shareware and freewares.
- Downloading, copying, otherwise duplicating, and/or distributing copyrighted materials without the specific written permission of the copyright owner, as specified in policy 2025 on copyright.
- Using electronic resources to access, process, or transmit obscene or pornographic content, sexually inappropriate content, or files dangerous to the integrity of the network. Malicious use of the electronic resources to develop programs that harass other users or infiltrate a computer or computing system and/or damage the software components of a computer or computing system.
- Making audio or video recordings or any facsimile of any person without their permission.
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing.)
- Any attempts to defeat or bypass the District's Internet filter by using or trying to use

proxies, https, special ports, modification to District browser settings or any other techniques, designed to avoid being blocked from inappropriate content or to conceal Internet activity; and
- Using any electronic resources for unlawful purposes and action that result in unapproved liability or cost incurred by the District.

Artificial Intelligence
Artificial Intelligence is a rapidly advancing set of technologies for capturing data to detect patterns and automate decisions. Artificial Intelligence (AI) has become an increasingly important part of our lives, and it is essential for students to understand when and how to use it effectively and ethically. AI tools can enhance classroom learning, and their implementation should be guided with proper training, ethical considerations, and responsible oversight. When utilizing generative AI tools to create or support the creation of texts or creative works, students are expected to adhere to these guidelines, and any additional guidance provided by their classroom teacher.

Purpose
The district will seek to maintain staff and student access to generative Artificial Intelligence tools for the following purposes:
- Ensuring all students have equitable access to leverage these technologies, regardless of what learning technology devices may be available to them.
- Providing all students with an opportunity to engage in current technologies in a learning environment, to better prepare them for the world they will live and work in.
- Extending the benefits of these tools to the workplace, where appropriate, to leverage efficiencies and productivity.

Appropriate Use
Student and staff use of generative Artificial Intelligence technologies should be used to support and extend student learning and workplace productivity. Student and staff use of AI will be in accordance with the expectations outlined in Policy 2022, this document (2022P), and the AI Code of Conduct.

Inappropriate Use
In addition to those uses that violate this procedure, the following are prohibited uses of Artificial Intelligence:
- Any use of Artificial Intelligence that does not align with expectations outlined by a classroom instructor or building administrator. It is ultimately the teacher's responsibility to determine the appropriate level of use of Artificial Intelligence in each classroom, and

for each assignment or project.
- Use of Artificial Intelligence to complete an assignment in a way that represents the assignment as one's own work.
- Use of Artificial Intelligence to purposefully create misinformation or to misrepresent others for the purpose of harming or bullying groups or individuals.
- Use of Artificial Intelligence with confidential student or staff personally identifiable information.

NETWORK SECURITY AND PRIVACY

The District network includes wired and wireless computers and peripheral equipment, files and storage, email and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The District utilizes filtering software to block and/or filter access to obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). The District reserves the right to prioritize the use of, and access to, the network. All use of the network must support education and research and be consistent with the mission of the District. Use of the computer network and Internet is a privilege, not a right. A user who violates this agreement shall, at a minimum, have his or her access to the network temporarily terminated. The District may also take other disciplinary actions as appropriate.

Annually, it is assumed that parents grant their child the right to access the network/equipment and have a desire to have their child use the Internet as an educational resource.

Annually, students will receive grade level instruction on digital citizenship and Internet Safety educating them about appropriate online behavior, using personal mobile devices at school, interacting with other individuals on social networking websites and cyberbullying awareness and response.

Students and staff are responsible for all activity on their account and must not share their account password. 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. To safeguard network user accounts , all users must adhere to the electronic and physical security procedures outlined in procedure 6501P - Data Privacy Procedures.

PUBLIC RECORDS

Because the Sumner-Bonney Lake School District is a public agency under the Washington Public Records Act, chapter 42.56 RCW, any information or record relating to the conduct of government or the performance of any governmental functions that is prepared, owned, used, or retained by the district is a public record subject to disclosure upon request by any person. Such

information may include retained records related to communications by or through District resources or records of Internet activity accessed by or through District resources. Whether such records, or any portion of such records, fall within the narrow exemptions of the Public Records Act will be determined once a request is received.

COPYRIGHT COMPLIANCE, related to Policy 2025
Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

All work completed by employees as part of their employment will be considered property of the District. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

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. If under an agreement with the District, the work will be considered the property of the District. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

STUDENT PRIVACY
The Children's Online Privacy Protection Act (COPPA) is a federal law, enacted in April 2000, related to the online collection of personal information from students under age 13. COPPA makes it clear to website owners what they must include in their privacy policy, when they must seek consent from parents for a child under 13 to use their services, and what the website owner's responsibilities are to protect the online privacy and safety of children. These rules apply regardless of whether the website is fee-based or not. COPPA does not preclude schools from acting as intermediaries between operators and parents in the notice and consent process, or from serving as the parent's agent in the process of collecting personal information online from students in the school context when parents have provided permission for student Internet use.

AI and COPPA:This includes information collected through the use of AI tools in educational settings. As outlined in this policy, where permitted under COPPA, the district may provide consent on behalf of parents for students under 13 to use online services, including AI tools,

when such services are used solely for educational purposes and for the benefit of the school. The district will adhere to the principles of data minimization, collecting only the minimum necessary student data for the specific educational purpose.

The District's use and sharing of student data is solely for education purposes. District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).This includes:

- **Maintaining Confidentiality:** All student education records, whether in electronic or paper format, will be handled confidentially and in accordance with FERPA regulations.
- **Limiting Access:** Access to student records will be limited to authorized individuals with a legitimate educational interest
- **Safeguarding Data:** The district will implement security measures to protect student data from unauthorized access, use, or disclosure, including data used in AI systems.

EMAIL AND INTERNET COMMUNICATIONS

Email and other Internet communication tools such as blogs, wikis and social networks are provided by the District for your professional and educational use. These systems are not to be used for extensive or ongoing personal communications. Internet communications are most effective when they have clarity, conciseness, and courtesy.

Student use of District-Sponsored Email and Collaborative Account

Sumner-Bonney Lake School District recognizes the value of online communication and collaboration both in and out of the classroom. Email accounts play a vital role in education as a mechanism for account sign up and teacher/student communication. Sumner-Bonney Lake School District is committed to allowing responsible, learning-centered use of district-sponsored email and collaborative accounts.

- Students may use district-sponsored email and collaborative accounts as directed by the teacher.
- Students will use their accounts responsibly. Students and parents understand district guidelines pertaining to the use of digital communications.
- Email and other electronic resources are not private. The Sumner-Bonney Lake School District is a publicly-funded organization accountable to public records requests and open record laws. WAC 434-662 - Preservation of Electronic Public Records

Separate Professional and Personal Email Accounts

District employees who decide to engage in professional social media activities should maintain separate professional and personal email addresses. As such, District employees should not use

their personal email address for professional social media activities. The professional social media presence should utilize a professional email address and should be completely separate from any personal social media presence maintained by the District employee. Regular and continuous use of a personal email address for professional purposes, including social media use, will result in the District considering the email address, and the corresponding use of that address, as a professional account.

SOCIAL MEDIA

Social Media Guidelines
In the fast-changing world of electronic information and communication with **families**, staff, and community members, the Sumner-Bonney Lake School District recognizes that social media tools can be of great value in furthering the District's mission and promoting the Board of Directors' goals. Schools and departments may be authorized to utilize social media in a manner consistent with state and federal law, Policy 2022 and 5254. The purpose of authorized social media sites is limited to promoting the mission and goals of the District.

Online communication is critical to our students' learning. Social media, web-based or Internet tools such as blogs, wikis, social networks, podcasts, email, or other Internet tools offer an authentic, real-world vehicle for student expression. Our primary responsibility to students is their safety. Hence, the District holds those staff and students, using these tools to the same responsible use, terms of agreement, standards and expectations and must follow all established Internet safety guidelines. Furthermore, if you are going to use these tools in your official capacity the District reserves the right to monitor appropriate behavior and adherence to instructional guidelines. Anything deemed to be inappropriate will be subject to deletion.

Professional Social Media Sites
District employees who use professional social media sites should follow these guidelines, along with policy 5254 Staff Use of Social Media**:.**

All District employees should treat professional social media space and communication like a professional workplace. The same standards expected in District professional settings are expected on professional social media sites. If a particular type of behavior is inappropriate in the classroom or a professional workplace, then that behavior is also inappropriate on the professional social media site;

All District employees should exercise caution, sound judgment, and common sense when using professional social media sites, as noted in Policy 5012 Civility in the Workplace**.~~;~~**

1. Setting up professional social media accounts and use

- Professional social media accounts must include language identifying the account as a school/department/club account, and must include the district's terms of use.
- District employees must use privacy settings and content moderation on their professional social media sites. Employees should be aware that there are limitations to privacy and content moderation settings, and they have a responsibility to understand the rules of the social media site being utilized.
- Everything published on the district's social media accounts are considered public records and can be requested as part of the Public Records Act (RCW 42.56).
- Professional social media sites that are school-based should be designed to address reasonable instructional, educational or extracurricular program matters and approved by supervisor;
- To the extent possible, based on the social media site being used, District supervisors or their designees should be given administrator rights or access to the professional social media accounts established by District employees;
- Professional social media communication should be in compliance with existing District policies and applicable federal and state laws, including, but not limited to, prohibitions on the disclosure of confidential information and prohibitions on the use of harassing, obscene, discriminatory, defamatory or threatening language;

1. Student information and privacy

- No personally identifiable student information may be posted by District employees on professional social media sites, including student photographs, without the consent of the students' parents/**guardians**; and
- **District employees must check the opt-out list in Skyward to determine whether a student may be photographed/recorded/quoted;**
- Students who **assist with** professional social media sites may not be permitted to post photographs, audio or video products featuring other students.

3. Monitoring and maintaining professional social media sites/accounts

- Employees using professional social media have no expectation of privacy with regard to their use of such media. The District will regularly monitor professional social media sites to protect the school community**.**
- It is the responsibility of the employee to routinely monitor their professional social media account(s) to review comments and activity, and to ensure that it adheres to district posting guidelines.
- District supervisors reserve the right to remove, disable, and provide feedback regarding

professional social media sites that do not adhere to District policy, the law, or that do not reasonably align with these guidelines**;.**

- District employees are mandated reporters and are required to abide by the same reporting responsibilities in a social media context.

4. Media inquiries

- Any media inquiries received via professional social media sites should be promptly referred to the Communications Office.

Personal Social Media Sites/Accounts

District employees should exercise caution and common sense when using personal social media sites**.**

Online activities should not interfere with your job duties. Personal social media use, including off-hours use, has the potential to result in disruption at school and/or the workplace, and can be in violation of District policies and federal and/or state law. Personal use of social media during district time or on district equipment should be quick and infrequent.

1. Communication with students

- In order to maintain a professional and appropriate relationship with students, district employees will not communicate with students who are currently enrolled in district schools on personal social media sites. This is subject to the following exceptions:
- Communication with relatives
- Pre-existing relationships
- In these instances, employees should notify their principal/supervisor.

2. Guidance regarding social media accounts

- The posting or disclosure of personally-identifiable student information or confidential information via personal social media sites, in violation of these guidelines is prohibited
- District employees are encouraged to use appropriate privacy settings to control access to their personal social media sites/accounts. Employees should be aware that there are limitations to privacy settings, and they have a responsibility to understand the rules of the social media site being used. Private communication published on the internet can easily become public.
- District employees should not “tag” photos of other District employees, District

volunteers, District contractors or District vendors without the prior permission of the individuals being tagged;

- District employees should not use the District's logo in any personal postings and should not link to the District's website or post District material on any personal social media sites without the permission of a District administrator. This does not include sharing or reposting posts from official district accounts.
- District employees should not use their personal social media accounts to act as representatives of Sumner-Bonney Lake School District.
- District employees are mandated reporters and are required to abide by the same reporting responsibilities in a personal social media context.
- The district does not actively monitor its employees' personal social media accounts. Should the district's attention be brought to an employee's personal social media content that demonstrates insubordination, immorality, cruelty, discrimination or other unlawful acts, the employee may be subject to disciplinary action.

District-Authorized Social Media

District staff will be authorized to access authorized social media sites during work hours in support of the educational mission and goals of the district. District staff may not initiate an authorized social media site for a school, department, class, activity, sport, or club unless expressly authorized to do so by the Superintendent or the Superintendent's designee. All staff employees using authorized social media sites will adhere to all District policies and procedures. The inappropriate use of social media by district employees is a violation of this procedure.

Authorized social media sites are not intended to be used for policy decisions or items of legal and fiscal significance that have not been previously disclosed to the public. To avoid conflicts with Washington's Open Public Meetings Act, chapter 42.30 RCW, the Board of Directors will not engage in meetings or discussions via authorized social media sites. Posting content via authorized social media sites does not constitute giving official or lawful notice to the district as may be required.

The District may choose to allow user-generated content on its social media sites. By doing so, however, the District is not creating an open public forum. The purpose of such sites is to inform and engage with students and their families, staff, residents and other members of our community while promoting the mission of the District and the Board of Directors' goals. Although comments will not be removed based on viewpoint, comments and observations must be civil, constructive, respectful, and responsible. Because the District has a compelling interest in the lawful use of public resources and maintaining content that is appropriate for all users, the following content will not be permitted on social networking sites administered by the

Sumner-Bonney Lake School District.

The SBLSD reserves the discretion to hide and remove comments, as well as block offenders, as a result of any social media user comments on any account operated by SBLSD - including, but not limited to, shared posts, replies, links, and/or images - that are inconsistent with the following guidelines:

- Content that promotes, fosters, or perpetuates discrimination on the basis of sex, race, color, religion, creed, national origin, sexual orientation, gender identity, gender expression, disability, age, and/or honorably discharged veteran or military status.
- Personal attacks, name-calling, harassing, or defamatory statements, including derogatory comments directed at another individual or group of individuals.
- Violent, obscene, profane, pornographic, or threatening content and/or language.
- Advocacy of or opposition to any political candidate, political party, or ballot measure.
- External content not suitable for readers or viewers of all ages.
- Promotion of or inciting illegal or violent conduct.
- Content that is off-topic.
- Content containing false or misleading information, such as misinformation and disinformation.
- Advocacy of, promoting, or discussing commercial activity or private business interests, including links to or advertising commercial activity
- Content that infringes on any trademark, copyright, or patent rights of another.
- Personal information including, but not limited to, email addresses, telephone numbers, mailing addresses, or personal identification numbers.
- Repetitive user comments, including those that are copied and pasted.

Comments, observations, and other postings in violation of these guidelines will be removed by the District. Opinions expressed by third parties on authorized sites are not those of the Sumner-Bonney Lake District or its employees. Because the school district is a public agency, all comments posted on social networking sites administered by the district are public records that will be archived and subject to disclosure upon request.

Authorized sites will not be available for public comments or observations unless staff members have been designated to regularly monitor postings and verify compliance with District policy and procedure. District staff so designated will monitor public comment and observations on an established, regular schedule and will remove content in violation of 2022 and 2022P. All removed content will be archived as a public record.

Adopted 3/2009
Revised 1/2018; **02/2025**

PERSONAL MOBILE DEVICES

Sumner-Bonney Lake School District recognizes that personal mobile devices are now an integral part of our community, culture and way of life. It is also recognized that these personal devices will play a significant part in education. Therefore, in accordance with all District policies and procedures, students, staff, parents and our community may use personal electronic devices while on District property to further the educational and research mission of the District. District and school administration will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day.

General Conditions for Personal Mobile Device Use

- The term personal mobile device in this policy denotes smartphones, mobile phones, laptops, notebooks/netbooks, eReaders, MPS3 or game players, iOS devices, tablets, cameras or any similar mobile device that can access the Sumner-Bonney Lake School District network and/or the Internet.
- All provisions, guidelines and procedures in Sumner-Bonney Lake School District Policies apply to all personal mobile devices connected to the District's network whether or not permission was granted.
- Parents or guardians must grant permission before their students can bring personal mobile devices to school whether the device will be used for emergency, personal and/or educational use.
- It is assumed students who bring any personal mobile device on District property have been granted permission to do so from their parents or guardians and agree to follow the responsible use procedures for personal mobile devices.
- Parents or guardians not granting permission for their student to use personal mobile devices on District property must notify the school in writing to the Principal or their designee.
- The responsible use procedures for mobile devices also apply to students during school excursions, camps and extracurricular activities.
- The use of a personal mobile device by staff, students, parents or community members on District property must adhere to the District's responsible use procedures for mobile devices as well as all provisions of the Electronic Resources Policy and Procedures.
- Failure to follow these responsible use procedures may subject staff or students to the District's Code of Conduct and may result in disciplinary action.

District's Responsibilities to Support Use of Personal Mobile Devices

- The District will provide a safe, monitored and filtered wireless network according to the Children's Internet Protection Act for students to use with their personal mobile devices. • If the District has reasonable cause to believe the student has violated the AUP or District

policies, authorized personnel may search a student's mobile device.

- Any use of the personal mobile device that is deemed a criminal offense, will be dealt with as such by the District.
- The District may remove the user's access to the network and suspend the right to use the personal mobile device if it is determined that the user is engaged in unauthorized or illegal activity or is violating the Electronic Resources policy and procedures.
- District staff will reasonably monitor and supervise students.
- The District will educate students in identifying, promoting, and best practices, good digital citizenship and Internet safety specifically for personal mobile devices.
- The District assumes no liability or responsibility for students that misuse mobile devices while on school property.
- The District accepts no financial responsibility for damage, loss, theft or costs associated with the use of the personal mobile devices while at school.

Responsible Use by Students

- Students will take complete responsibility for their personal mobile devices while at school.
- Students will keep the mobile device secure and locked away when not in use and never leave it in any open area unattended.
- Each school will determine specific acceptable use of a personal mobile device. • School staff will determine the appropriate use of personal mobile devices for students, and have the right to allow or disallow the use during instructional time in the classroom. • School staff has the right to determine whether personal mobile devices are stored out of sight or placed on the student's desk in plain sight.
- Student's personal mobile devices with Internet access capabilities are expected to access the Internet through the school's filtered network while on school property.
- Student's personal mobile devices will never be used in any manner or place that is disruptive in a classroom, school, or while participating in any other activity in the District.
- Using personal mobile phones or devices to bully and threaten other students is unacceptable and will not be tolerated.
- Pictures and videos must not be taken of students, teachers or other individuals without their permission.

Personal Device Warning

By connecting a mobile device to the Sumner-Bonney Lake School District systems, you acknowledge and agree that the Sumner-Bonney Lake School District Technology Services Department reserves the right to enforce any reasonable security measures deemed necessary to mitigate data leakage and protect students. This includes but is not limited to:

- Devices that have access to District email, student information system or other District resources must have a secure pass lock;
- Deleting the contents of your mobile device when deemed necessary, e.g., when a password is incorrectly entered more than 10 times. The deletion may include district and personal contacts, pictures, etc.; and
- Restricting the use of applications deemed a security risk.

In addition, users of district networks with personal devices understand that documents or records prepared, owned, used, or retained by any local or public agency – including the electronic communications of a public agency—are public records under Washington state law. Using any personal device or computer for school district business can result in a requirement that you submit your personal device for examination or search if a public records request is received concerning information related to governmental conduct or the performance of any governmental function that may be stored on your personal device.

LEGAL NOTICES

The Sumner-Bonney Lake School District is not responsible for the information that is retrieved via electronic resources.

Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications. Network administrators have access to all email and will monitor messages.

Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

The District reserves the rights to monitor, inspect, copy, review, and store without prior notice any and all usage of: the network; user files and disk space utilization; user applications and bandwidth utilization; user document files, folders, and electronic communications; internet access; and any and all information transmitted or received in connection with network and/or email use operated by or through District resources.

All information files shall be and remain the property of the District, and no student or staff user shall have any expectation of privacy regarding such materials. The District reserves the right to disclose any electronic message to law enforcement officials or third parties as deemed appropriate. All documents generated, received, transmitted, or maintained through district

resources or networks are subject to the disclosure laws of the State of Washington's Public Records Act, chapter 42.56 RCW.

Backups are made of email for the purpose of public disclosure requests and disaster recovery. Barring power outages or intermittent technical issues, tape backups are made of staff and student files on District servers for recovery of accidental loss of deleted files. Recovery is not guaranteed.

While filtering software makes it more difficult for objectionable material to be received or accessed through District resources, filters are not infallible. The ability to access a site does not mean that otherwise objectionable material or an objectionable site falls within the District's responsible use requirements. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites and/or materials. Any inadvertent visit to an objectionable site must be reported immediately.

From time to time, the Sumner-Bonney Lake School District will make determinations on whether specific uses of electronic resources are consistent with the District Electronic Resources policy.

The Sumner-Bonney Lake School District will not be responsible for any damages users may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions caused by our own negligence or user errors or omissions. Use of any information obtained is at the user's own risk.

The Sumner-Bonney Lake School District makes no warranties (expressed or implied) with respect to:

• The content of any advice or information received by a user or any costs or charges incurred as a result of seeking or accepting any information.
• Any costs, liability, or damages caused by the way the user chooses to use his or her access to the electronic resources.

The Sumner-Bonney Lake School District reserves the right to change its rules and procedures at any time without notification. 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 implementation will be made available for administration, staff, and families.

Adopted 3/2009
Revised 1/2018; **02/2025**

VIOLATIONS OF RESPONSIBLE USE PROCEDURES
Any reasonable belief that user activity has violated this policy and procedure regarding responsible use should be reported to the school, program, or department administrator responsible for supervision of the use in question. Disciplinary action, if any, for students, staff, and/or other users shall be consistent with the District's policies and procedures.

Violations of this policy can constitute reasonable cause for the limitation or revocation of access privileges, or suspension of access to Sumner-Bonney Lake School District electronic resources. Violations may also result in employee discipline for staff or school disciplinary action for students, as well as other appropriate legal or criminal sanctions, as appropriate.

CHALLENGING THE DENIAL OR RESTRICTION OF ACCESS TO DISTRICT ELECTRONIC RESOURCES
If a person is denied access or subject to restricted access to the District's electronic resources resulting from a determination that the person has violated the District's responsible use standards, the denial or restriction may be appealed.

If access to electronic resources is denied or restricted for a student, the denial or restriction may be grieved consistent with the procedures for student discipline contained within policy 3241 and as set forth in WAC 392-400-240. If access to electronic resources is denied or restricted for a student as part of a suspension or expulsion, the denial or restriction may be challenged consistent with the procedures and provisions of 3241P and chapter 392-400 WAC applicable to the suspension or expulsion imposed.

Reference Policies or Procedures:
2022, 2025, 3207, 3241P, 5011, 5011P, 5012, 5253, 5253 P, 5254, 6501, 6501P

Legal Documents:
18 USC §§ 2510-2522 - Electronic Communication Privacy Act
20 USC 6801 et seq. - Elementary and Secondary Education Act
47 USC 254 - Universal Service Children's Internet Protection Act (CIPA)
15 USC 6501-6508 - Children's Online Privacy Protection Act (COPPA)
20 USC § 1232g; - Family Educational Rights and Privacy Act (FERPA)
34 CFR Part 99 - Family Educational Rights and Privacy Act (FERPA)
17 USC - United States Copyright Law
WAC 434-662 - Preservation of electronic public record

Adopted 3/2009
Revised 1/2018; **02/2025**