Procedure: Electronic Resources and Internet Safety

Acceptable Use Guidelines/Internet Safety Requirements
These procedures are written to support the Electronic Resources and Internet Safety Policy of the Board and to promote positive and effective digital citizenship among students and ESD 112 employees. Digital citizenship includes the norms of appropriate, responsible, and healthy behavior related to current technology use.

Successful, technologically-fluent digital citizens recognize and value the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world. They recognize that information posted on the Internet can have a long-term impact on an individual's life and career. They cultivate and manage their digital identity and reputation, and are aware of the permanence of their actions in the digital world. Expectations for student and employee behavior online are no different from face-to-face interactions.

Use of Personal Electronic Devices
Students and employees are furnished technology equipment by ESD 112 or by the school district in which employees are assigned, based on their role and the appropriate level of access to these tools. In general, these are the extent to which technology equipment should be used for ESD 112/district-related school/work. Employees serving in districts using district-equipment shall follow the district's policies, procedures, and operating practices for use of that equipment. ESD 112 employees will retain the authority to decide when and how students may use personal electronic devices on school grounds and during the school day. Employees' use of personal devices on the ESD 112 network is limited as follows:

- Employees are restricted from accessing ESD 112 resources such as district printers, network folders, and ESD 112-hosted servers on their personal devices. Other uses, such as access to the ESD 112's internet connection from personal devices is subject to available resources and may be limited.
- Employees will use ESD 112-issued devices, not personal devices, for accessing district and student data.
- Personal electronic devices will be connected to the ESD 112 network only by Wi-Fi, not by cable. All personal electronic devices must have up-to-date virus prevention software and current operating systems patches. Browsers must also be updated to the most current version.

Network
The ESD 112 network includes wired and wireless devices and peripheral equipment, files and storage, e-mail, and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The ESD 112 reserves the right to prioritize the use of, and access to, the network.

All use of the network, as well as any materials stored, transmitted, or published on the system, must be in conformity to state and federal law-including FERPA and CIPA, network

provider policies and ESD 112 policy. All use of the network must support education and research and be consistent with the mission of ESD 112.

From time to time, ESD 112 may determine whether specific uses of the network are consistent with the regulations stated in this procedure. Under prescribed circumstances, non-student or employees use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of ESD 112.

For security and administrative purposes, ESD 112 reserves the right for authorized personnel to review system use and file content including, without limitation, the contents of ESD 112 provided personal and shared file storage, web browsing history on an ESD 112 device and/or the ESD 112 network, and ESD 112 email. Email is archived as per Public Disclosure Laws.

Acceptable network use by ESD 112 students and employees include:

A. Creation of files, digital projects, videos, web pages, and podcasts using network resources in support of education and research;
B. Participation in blogs, wikis, bulletin boards, social networking sites and groups as permitted under ESD 112 filtering limitations, and the creation of content for podcasts, e-mail, and webpages that support education and research;
C. With parental permission, the online publication of original educational material, curriculum-related materials, and student work. Sources outside the classroom or school must be cited appropriately;
D. Employees use of the network for incidental personal use in accordance with all ESD 112 policies and procedures; or
E. Connection of personal electronic devices (wired or wireless), when authorized, including portable devices with network capabilities, to the ESD 112 network that is equipped with up-to-date virus software, compatible network card, and is configured properly. Connection of any personal electronic device is subject to all procedures in this document and ESD 112 policy.

Unacceptable network use by ESD 112 students and employees includes but is not limited to:

A. Personal gain, commercial solicitation, and compensation of any kind;
B. Actions that result in liability or cost incurred by the ESD 112
C. Downloading, installing and use of games, audio files, video files, games, or other applications (including shareware or freeware);
D. Support for or opposition to ballot measures, candidates, and any other political activity;
E. Hacking, cracking, vandalizing, the introduction of malware, including viruses, worms, Trojan horses, time bombs, and changes to hardware, software, and monitoring tools;
F. Making use of the electronic resources in a manner that serves to disrupt the operation of the system by others, including modifying, abusing, or destroying system hardware, software, or other components.
G. Attempting to gain or achieving unauthorized access to other ESD 112 computers, networks, and information systems;
H. Action constituting or contributing to harassment, intimidation, or bullying, including cyberbullying, hate mail, defamation, discriminatory jokes, and remarks. This may also include the manufacture, distribution, or possession of inappropriate digital images;

I. Information posted, sent, or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
J. Accessing, uploading, downloading, storage and distribution of obscene, pornographic, or sexually explicit material;
K. Attaching unauthorized devices to the ESD 112 network. Any such device will be confiscated, and additional disciplinary action may be taken; or
L. Any unlawful use of the ESD 112 network, including but not limited to stalking, blackmail, violation of copyright laws, and fraud.

ESD 112 will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by his/her own negligence or any other errors or omissions. ESD 112 will not be responsible for unauthorized financial obligations resulting from the use of, or access to, ESD 112's computer network or the Internet.

Internet Safety Instruction
Employees will be educated regarding cybersecurity, including regular cybersecurity training as well as ongoing phishing simulations.

Personal Information and Inappropriate Content
A. Students and employees should not reveal personal information, including a home address and phone number on web sites, blogs, podcasts, videos, social networking sites, wikis, e-mail, or as content on any other electronic medium;
B. Students and employees should not reveal personal information about another individual on any electronic medium without first obtaining permission;
C. No student pictures or names can be published on any public class, school, or ESD 112 website unless the appropriate permission has been obtained according to ESD 112 policy;
D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority;
E. No user may use, disclose, or disseminate personally identifiable information of a minor without explicit parent/guardian permission;
F. Employees must follow ESD 112 data-handling procedures, including Policy 3231 – Student records, when handling any student's personally identifiable information; and
G. Students should be aware of the persistence of their digital information, including images and social media activity, which may remain on the Internet indefinitely.

Filtering and Monitoring
Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

A. 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 themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
B. Any attempts to defeat or bypass the ESD 112's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to ESD 112 browser settings, and any other techniques designed to evade filtering or enable the publication of inappropriate content);

C. E-mail inconsistent with the educational and research mission of the ESD 112 will be considered SPAM and blocked from entering ESD 112 e-mail boxes;
D. ESD 112 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 ESD 112 devices;
E. Employees who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of ESD 112
F. Employees must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively;
G. ESD 112 may monitor student use of the ESD 112 network, including when accessed on students' personal electronic devices and devices provided by the ESD 112, such as laptops, netbooks, and tablets;
H. ESD 112 may block or delete any malicious content detected, and
I. ESD 112 will provide a procedure for employees to request access to internet websites blocked by the ESD 112's filtering software. The procedure will indicate a timeframe for a designated school official to respond to the request. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request. The ESD 112 will provide an appeal process for requests that are denied.

Copyright
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 is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Ownership of Work
All work completed by employees as part of their employment will be considered property of ESD 112. ESD 112 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 ESD 112, the work will be considered the property of ESD 112. Employees must obtain a student's permission prior to distributing his/her work to parties outside the school.

Privacy
ESD 112 employees must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

No Expectation of Privacy
ESD 112 provides the network system, e-mail, and Internet access as a tool for education and research in support of ESD 112's mission. ESD 112 reserves the right to monitor, inspect, copy, review, and store, without prior notice, information about the content and usage of:

A. ESD 112 network, regardless of how accessed;
B. User files and disk space utilization;

C. User applications and bandwidth utilization;
D. User document files, folders, and electronic communications;
E. E-mail;
F. Internet access; and
G. Any and all information transmitted or received in connection with network and e-mail use.

No student or employee user should have any expectation of privacy when using the ESD 112 network. ESD 112 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.

Hardware, Educational Applications, and Programs
Hardware, and all applications, including software, and operating systems must be approved for use prior to purchase and installation according to current technology purchase procedures. Additionally, hardware and all applications, software, and operating systems must be:

A. Currently supported by the manufacturer.
B. Periodically reviewed to ensure they are still in use, supported by the manufacturer, and patched for vulnerabilities.

ESD 112 will remove any hardware, application, software, or operating system that does not meet these criteria.

Application & Devices for Students
ESD 112 employees may request students to download or sign up for applications or programs on the students' personal electronic devices. Such applications and programs are designed to help facilitate lectures, student assessment, communication, and teacher-student feedback, among other things.

Prior to requesting students to download or sign up for educational applications or programs, the employee will review "terms of use," "terms of service," and/or "privacy policy" of each application or program to ensure that it will not compromise students' personally identifiable information, safety, and privacy. Specific expectations of use will be reviewed with students.

Employees should also, as appropriate, provide notice to students' parents/guardians that the employee has requested that students download or sign up for an application or program, including a brief statement on the purpose of application or program.

Archive and Backup
Backup is made of all ESD 112 e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outages or intermittent technical issues, employees and student files are backed up on ESD 112 servers regularly. Refer to the ESD 112 retention policy for specific records retention requirements.

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.

Disciplinary Action
All users of ESD 112's electronic resources are required to comply with ESD 112's policy and procedures and agree to abide by the provisions set forth in ESD 112's user agreement. Violation of any of the conditions of use explained in any of these documents could be cause for suspension or revocation of network, computer access, or other electronic resources privileges. Additionally, violations of these documents could result in disciplinary action, including suspension from school, termination of employment, and/or civil or criminal actions, as warranted.

Accessibility of Electronic Resources
In compliance with federal and state law, all ESD 112-sponsored programs, activities, meetings, and services will be accessible to individuals with disabilities, including persons with hearing, vision, and/or speech disabilities. To ensure such, the content and functionality of websites associated with the ESD 112 should be accessible. Such websites may include, but are not limited to, the ESD 112's homepage, teacher websites, ESD 112-operated social media pages, and online class lectures.

ESD 112 employees with authority to create or modify website content or functionality associated with the ESD 112 will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities. Any such employee with questions about how to comply with this requirement should consult with the Executive Director of Communications.

ADOPTION DATE: **10-28-2025**