Procedure - Electronic Resources and Internet Safety

1.0 Scope

These procedures are written to support the Electronic Resources and Internet Safety Policy of the Wenatchee School Board of Directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship includes the norms of appropriate, responsible, and healthy behavior related to current technology.

The following procedures apply to all Wenatchee School District (hereby referred to as "District") staff, students, and guests, or anyone with a district provided device or account that is using our resources; and cover all district technology, network access, and software licensed to the district.

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 staff behavior online are no different from face-to-face interactions.

2.0 Appropriate Use

The District expects everyone to exercise mature judgment and use District technology in a professional manner. The Superintendent reserves the right to define mature judgment and/or professional manner. Use of the technology is expected to support the District's goals of educating students and/or conducting District business. The District recognizes, however, that some personal use is inevitable. Therefore, incidental and occasional personal use that is infrequent or brief in duration is permitted so long as it occurs on personal time, does not interfere with District business, and is not otherwise prohibited by District policy or procedures.

2.1 Use of personal electronic devices

In accordance with all District policies and procedures, students and staff may use personal electronic devices to further the educational and research mission of the District. 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. Absent a specific and articulated need (e.g. assistive technology), students do not have an absolute right to possess or use personal electronic devices at school.

Since the Wenatchee School District supplies devices and accounts to use for district business we discourage employees' and officials' use of home computers, personal devices or personal accounts for agency business. If any home computers, personal devices or personal accounts are used for district business we have the obligation to request the retrieval of public records from these devices and accounts. The use of personal email accounts should never be used for district business and forwarding district email to a personal account will leave a record of the communication within district systems. In addition we recommend that if personal devices are used that the staff member only uses our adopted cloud based tools to ensure records retention without data being stored on their personal device. To increase the security of staff accounts we will ask that staff use their personal devices for multi factor authentication to ensure account security.

A. Staff are restricted from accessing district resources unless connected to the staff wifi network by enrolling their device with district credentials.
B. Staff will use district-issued devices, not personal devices for accessing district and student identifiable information unless that information is contained within the district cloud services and not copied to the personal device.
C. Personal electronic devices will be connected to the district network only by Wi-Fi, not by cable. The staff personal device must enroll using their district credentials and will be subject to stricter internet filtering depending on their location. 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.

2.2 Use of the District Network

The District network includes wired and wireless devices and peripheral equipment, files and storage, email and Internet content. 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.

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 district policy. All use of the network must support education and research and be consistent with the mission of the district.

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

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

Acceptable network use by District students and staff include:

A. Creation of files and digital projects using network resources in support of education and research;
B. Participation in blogs, wikis, bulletin boards, social networking sites and

groups and the creation of content for podcasts, email, and web pages that support education and research;

C. With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources used from outside the classroom or school must be cited appropriately;

D. Staff use of the network for incidental personal use in accordance with all District policies and procedures; or

E. Connection of personal wireless electronic devices including portable devices with network capabilities to the District's guest network or staff personal phones to the staff network using the Districts WiFi self enrollment. At no time may a hard wired connection be made to the network without the explicit permission of the the Director of Technology. Connection of any personal wireless electronic device is subject to all procedures in this document.

Unacceptable network use by District students and staff 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 District;

C. Downloading, installing and use of games, audio files, video files, or other applications (including shareware or freeware) that conflict with District systems and policies.

D. District technology may not be used to interfere or disrupt other users, services, or equipment. Disruptions include distribution of unsolicited advertising ("spam"), and distribution of large quantities of information that may overwhelm the system (chain letters, network games, or broadcasting messages), and any unauthorized access to, or destruction of, District technology or other resources accessible through the District's network.

E. Support for or opposition to ballot measures, candidates and any other political activity. Using District technology for political purposes in violation of federal, state, or local laws are prohibited. This prohibition includes the use of District technology to assist or to advocate, directly or indirectly, for or against a ballot proposition and/or the election of any person to any office. The use of District technology for the expression of personal political opinions to elected officials is prohibited. Only those staff authorized by the Superintendent may express the District's position on pending legislation or other policy matters.

F. Hacking, cracking, vandalizing, the introduction of viruses, malware, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;

G. Unauthorized access to other District technology, networks and information systems, including any violation of the purpose and goal of the network, network security, or content filter, and/or the intent to bypass either the District border firewall or content filter;

H. 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;

I. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks. Harassment includes slurs, comments, jokes, innuendoes, unwelcome compliments, cartoons, pranks, or verbal conduct relating to an individual that (1) have the purpose or effect of creating an intimidating, hostile, or offensive environment; (2) have the purpose or effect of unreasonably interfering with an individual's work or school performance; (3) have the purpose or effect of defamation of staff; and/or (4) interfere with school operations.

J. Information posted, sent or stored online that could directly or indirectly endanger others;
K. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material. Using District technology for inappropriate or indecent purposes (including accessing, storing, or viewing pornographic, indecent, or otherwise inappropriate material), or in support of such activities, is prohibited. Indecent activities include violations of generally accepted social standards for use of publicly owned and operated equipment;
L. Attaching unauthorized devices to the Districts non-guest network via a hard wired connection. Any such device will be confiscated and additional disciplinary action may be taken;
M. Illegal activities include any violations of federal, state, or local laws (for example, infringing on copyright, publishing defamatory information, or committing fraud);
N. Vandalism, including any attempt to harm or destroy operating systems, application software, hardware, or data.
O. Any unlawful use of the district network, including but not limited to stalking, blackmail, violation of copyright laws, and fraud.

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, mis-deliveries 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 network or the Internet.

2.3 Use of District Software

District software is licensed to the District by a number of vendors that may have specific licensing restrictions regarding duplication or use of a particular program. Users of District software must obtain permission from the District prior to copying or loading District software onto any technology, whether the technology is privately owned or owned by the District. The use of a District owned Apple ID, Filewave Kiosk, and Wenatchee School Google store will be the only method for user installation of approved software.

Users are not to delete or add software to District technology without District permission. Due to diverse licensing terms for different software programs, users should *not* assume that if it is permissible to copy one program, then it is permissible to copy others.

2.4 Remote Email Access

The District provides access to District email via the Internet for the convenience of its staff. The District also provides access to personal email from within the District network only through web access.

2.5 District approved cloud services

District cloud services may be used only by District staff, students and others expressly authorized by the District to use the service. Everything within this procedure must be adhered to when using District approved cloud services. Approved cloud services are those that have an agreement with the District to store data outside the District network.

2.6 Non-District Employee Use

District technology may be used only by District staff, students and others expressly authorized by the District to use the equipment.

2.7 Public Records

The District is obligated to retain, search, recover, and provide any record pertaining to District business from any District device or account, and where applicable from any personal accounts or devices used for conducting District business according to WAC 44-14-03001(3).

3.0 Internet Safety and Personal Information

Lessons on online safety issues and cyberbullying awareness/response will be provided at least annually and updated each year. All students will receive a short, age-differentiated lesson on the meaning of the contents of the district acceptable use policy.

Staff will be educated regarding cybersecurity, including periodic cybersecurity training as well as ongoing phishing simulations.

District technology, the Internet, and use of email are not inherently secure or private. For example, the content of an email message, including attachments, is analogous to a letter or official memo rather than a telephone call since a record of the contents of the email may be preserved by the sender, recipient, any parties to whom the email may be forwarded, or by the email system itself. It is important to remember that once an email message is sent, the sender has no control over where it may be forwarded and that deleting a message from the user's computer system does not necessarily delete it from the District system. In some cases, emails have also been treated as public records in response to a public records disclosure request. Likewise, files such as Internet "cookies" may be created and stored on a computer without the user's knowledge. Users are urged to be caretakers of their own privacy and not to store sensitive or personal information on District technology. The District may need to access, monitor, or review electronic data stored on District technology, including email and Internet usage records.

A. Students and staff should not reveal personal information, including a home address and phone number on websites, blogs, podcasts, videos, social networking sites, wikis, email or as content on any other electronic medium;
B. Students and staff 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 District website unless the appropriate permission has been obtained using District consent forms;
D. If students encounter dangerous or inappropriate information or messages, they

should notify the appropriate school authority;

E. Students under the age of 13 may require parental consent, using District forms, to create accounts within online systems outside of the District, in accordance with the Children's Online Protection Act (COPPA);
F. Staff must follow district data-handling procedures, including 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.

4.0 Filtering and Monitoring

While the District respects the privacy of its staff, and while the District currently does not have a practice of monitoring or reviewing electronic information, the District reserves the right to do so for any reason. The District may monitor and review the information in order to analyze the use of systems or compliance with policies, conduct audits, review performance, obtain information, or for other reasons. The District reserves the right to disclose any electronic message to law enforcement officials, and under some circumstances, may be required to disclose information to law enforcement officials, the public, or other third parties; for example, such disclosure may be required in response to a request made in a lawsuit involving the District or by a third party against the user or pursuant to a public records disclosure request.

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 determined by the District.

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 in 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 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);
C. Email inconsistent with the educational and research mission of the District will be considered SPAM and could be blocked from entering District email boxes;
D. The District will provide age appropriate 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 and use of District technology;
E. Staff members who supervise students or have occasion to observe student use of technology, must make a reasonable effort to monitor use and assure that student use conforms to the mission and goals of the District;
F. Staff must make a reasonable effort to become familiar with current technology and to monitor, instruct and assist effectively;
G. The district may monitor student use of the district network, including when accessed on students' personal electronic devices and devices provided by the

district, such as laptops, netbooks, and tablets;

H. The district may block or delete any malicious content detected, and
I. The district will provide a procedure for students and staff members to request access to internet websites blocked by the district'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.

5.0 Internet Safety Instruction

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.

A. Age appropriate materials will be made available for use across grade levels.

B. Training on online safety issues and materials implementation will be made available for administration, staff and families. Links to instructional material can be found on the Technology website.

6.0 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.

7.0 Ownership of Work

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.

8.0 Network Security and Privacy

8.1 Network Security

Passwords are the first level of security for a user account. System login and accounts are to be used only by the authorized owner of the account for authorized District purposes. Students and staff 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:

A. Change passwords according to District or system policy;
B. Do not use another user's account;
C. Should not insert passwords into email or other communications;
D. If you write down your user account password, keep it in a secure location;
E. Do not store passwords in a file without encryption;
F. Should not use the "remember password" feature of Internet browsers; and
G. Lock the screen or log off if leaving the computer

8.2 Privacy

A. Student Data is Confidential
District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA),

8.3 No Expectation of Privacy

The District provides the network system and services as tools for education and research in support of the District's mission. The District reserves the right to monitor, inspect, copy, review and store without prior notice information about the content and usage of:

A. The district 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. Email;
F. Internet services;
G. Any and all information transmitted or received in connection with network and email use.

No student or staff user 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.

9.0 Educational Applications and Programs

District staff 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.

Prior to requesting students to download or sign up for educational applications or programs, staff 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. Staff will also provide notice in writing of potential use of any educational application or program that fits into this category by submitting a technology support ticket, including the anticipated purpose of such application or program. If approved for use, specific expectations of use will be reviewed with students prior to using the newly approved application or program.

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

10.0 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.

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

11.0 Archive and Backup

Backup is made of all District email correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are archived to District approved cloud services or District servers. Refer to the District retention policy for specific records retention requirements.

12.0 Disciplinary Action

The Acceptable Use Policy is applicable to all users of District technology and refers to all information resources utilized within that technology. All users of the District's electronic resources are required to comply with the District's policy and procedures (and agree to abide by the provisions set forth in the District's user agreement). Disciplinary action, if any, for students, staff, and other users shall be consistent with the District's standard policies and practices. Violation of any of the conditions of use explained in the Wenatchee School District user agreement, Acceptable Use Policy 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, and/or appropriate legal action. Specific disciplinary measures will be determined on a case-by-case basis.

13.0 **Care for District Technology**

Users of District technology are expected to respect the District's property and be responsible in use of the technology. Users are to follow any District instructions regarding maintenance or care of the technology. Users may be held responsible for any damage caused by intentional or negligent acts in caring for District technology under their control. The District is responsible for any routine maintenance or standard repairs to District technology. Recommendations for the care and cleaning of technology can be found on the Technology Department website. Users are expected to notify the District via a ticket or helpdesk of any need for service in a timely manner.

If District technology is lost, damaged, or stolen while under the control of a user, outside of the school District, the user is expected to file a claim under his/her insurance coverage, when coverage is available. When personal coverage is unavailable the user is expected to reimburse the District for repair or replacement at current market cost.

If District technology is lost, damaged, or stolen while under the control of a user, outside of the school District conducting official District business, and it is determined accidental, the District will cover repair/replacement expenses.

Except in cases of negligent or intentional loss or damage, the District may cover out-of-pocket expenses when approved by the district Technology Director when the device was being used appropriately for district business and an unforeseeable accident occurs. If the damage was caused by not following care and use guidance, then the user may be held liable for the damages.

14.0 **Accessibility of Electronic Resources**

Federal law prohibits people, on the basis of disability (such as seeing and hearing impairments), from being excluded from participation in, being denied the benefits of, or otherwise being subjected to discrimination by the district. To ensure that individuals with disabilities have equal access to district programs, activities, and services, the content and functionality of websites associated with the district should be accessible. Such websites may include, but are not limited to, the district's homepage, teacher websites, district-operated social media pages, and online class lectures.

District staff with authority to create or modify website content or functionality associated with the district will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities. Any such staff member with questions about how to comply with this requirement should consult with the district Technology Director

15.0 **Artificial Intelligence (Ai) And Other Emerging Technologies**

Our school district recognizes the importance of preparing students for the future by equipping them with the skills necessary to responsibly and ethically use Artificial Intelligence (AI) and other emerging technologies as tools to enhance their learning experiences. This policy aims to promote the responsible, ethical, and transparent use of AI technologies while maintaining the principle of a "human in the loop." The "human in the loop" principle refers to the essential involvement of human supervision, control, and decision-making in conjunction with AI technologies to ensure accountability, accuracy, oversight, and ethical use. When appropriate, students are encouraged to use AI tools to aid them in crafting their original work, demonstrating their learning and understanding, and adequately citing and/or documenting AI-generated content when applicable.

The primary goal of using AI in classrooms is to support and enhance teaching and learning, increase student engagement, and provide opportunities for students to develop essential skills needed to prepare them to be future-ready, including but not limited to information literacy, critical thinking, collaboration, creativity, and innovative problem-solving skills.

Current AI Applications and sites will be reviewed as the Technology Department is made aware and has capacity to do so. The current list of AI sites reviewed for use is located on the Technology Department website under District System Guidelines, this document will change often and is not guaranteed to have all the tools staff or students may encounter. If you encounter a tool that you would like reviewed please have a staff member request review by the Technology Department.

Student Responsibility and Transparency:

- Students are encouraged to use AI and other emerging technologies responsibly and transparently, understanding that these tools are meant to complement their educational journey.
- Students shall use AI tools in accordance with the district's policy and regulation regarding Acceptable Technology Use.
- Students shall not attempt to pass off AI-generated content as their own work. The use of AI tools should be for assistance and enhancement, not substitution.
- Students must be able to explain how they used AI tools to complete their work and demonstrate their own understanding of the material.
- Students will clearly communicate the role of AI tools used in creating original work by properly citing and/or documenting AI contributions according to assignment/task requirements.

Staff Expectations:

- Staff members are permitted and encouraged to use AI technologies to augment their professional practice, exercising and modeling the same level of responsible, ethical, and transparent use we expect from students.
- Staff should offer guidance on how ALL students can effectively use AI technologies to augment their learning experience and empower their autonomy, while preserving the originality of their work.

- Staff should monitor student use of AI tools to ensure that students are using them in a responsible and ethical manner.
- Staff are responsible for providing clear expectations regarding the use of AI tools in their courses.
- Staff shall specify when and to what extent the use of AI tools is approved for particular assignments, tasks, projects, or assessments.

Curriculum Integration:

- AI technologies may be integrated into the curriculum where applicable, aligning with educational standards and learning objectives.
- Staff are encouraged to explore innovative ways to incorporate AI tools into lesson plans and activities to promote active learning and critical thinking.

Prohibited Use of AI Detection Tools:

- The district believes that fostering a culture of trust, responsibility, and transparency is more effective than relying on AI detection tools, which may have limitations (including unreliable results) and can inadvertently discourage students from exploring AI's potential for learning.
- In an instance where cheating is suspected, staff should not elicit the assistance of AI for identifying academic dishonesty, but instead hold a conversation with the student and consider offering an alternative method or new attempt to demonstrate learning.

Privacy and Data Security:

- In accordance with district policy and all regulations protecting student data and educational records, staff and students will not share or enter students' Personally Identifiable Information (PII) in AI tools without administrative approval.
- The school district shall ensure that any AI tools approved for use by students for educational purposes comply with relevant privacy and data security regulations, protecting students' personal information and data.

Professional Development:

- The school district may provide professional development as it deems fit for staff to stay informed about and practice with the latest AI technologies and their educational applications, ensuring they are equipped to guide students effectively.

16.0 Accessibility of Electronic Resources

In compliance with federal and state law, all District-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 district should be accessible. Such websites may include, but are not limited to, the district's homepage, teacher websites, district-operated social media pages, and online class lectures.

District staff with authority to create or modify website content or functionality associated with the district will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities. Any such staff member with questions about how to comply with this requirement should consult with district technology or communciations department staff

Adoption Date: **5.15**
Classification:
Revised Dates: **8.18; 7.24**