INSTRUCTION

Electronic Information System, Electronic Resources, and Internet Safety

These procedures are designed 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 use.

Use of Personal Electronic Devices

In accordance with all district policies and procedures, students and staff may use personal electronic devices (e.g., laptops, mobile devices, and tablets) to further the educational and research mission of the district in accordance with Board policy. 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.

Network and District Provided Devices

The district network includes wired and wireless devices and peripheral equipment, files and storage, email, and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The district 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 the Family Educational Rights and Privacy Act (FERPA) and Children's Internet Protection Act (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.

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 in accordance with public records disclosure laws.

Acceptable Use

Acceptable network use by district students and staff includes:

A. Creation of files, digital projects, videos, web pages, and podcasts using network resources in support of education and research;
B. Participation in blogs, bulletin boards, social networking sites and groups as permitted under district filtering limitations, and the creation of content for podcasts, email, and webpages that support education and research; or
C. Staff use of the network for incidental personal use in accordance with all district policies and procedures.

Unacceptable Use

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, shareware or freeware (approval must follow the processes outlined in policy and procedure 2310 Selection and Adoption of Instructional Materials);
D. Support for or opposition to ballot measures, candidates, and any other political activity;
E. Hacking, cracking, vandalizing, the introduction of malware (e.g., viruses, worms, crypto lockers) 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 district 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 district network. Any such device will be confiscated, and additional disciplinary action may be taken; or
L. 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 negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district's computer network or the Internet.

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.

All students will receive grade level appropriate lessons on the meaning of the contents of the acceptable use policy (AUP) and annually sign the AUP. The purpose of obtaining student signatures is to indicate their understanding and agreement to follow the provisions of the AUP. Students will be educated regarding appropriate digital citizenship and media literacy.

Staff will be educated and trained as appropriate for their roles regarding cybersecurity.

Filtering and Monitoring

Filtering software is used to block or filter access to objectionable material and visual depictions that are obscene and all child pornography in accordance with CIPA.

A. Filtering software is not infallible. While filters make it more difficult for objectionable material to be received or accessed, filters are not a complete solution. All users must take responsibility for their 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 blocked from entering district email boxes.
D. The district will provide appropriate adult supervision of Internet use. Consistent and deliberate monitoring of student use of devices is critical in ensuring students are accessing appropriate material and not accessing inappropriate material on the Internet.
E. Staff members 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 the district.
F. Staff are responsible for becoming familiar with the Internet and electronic resources 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.

The district will provide a procedure for staff members to request access to Internet websites blocked by the district's filtering software.

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 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.

Security

System logins or accounts are to be used only by the authorized owner of the account for the authorized purpose.

A. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.
B. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users; misrepresent other users on the system, or attempt to gain unauthorized access to any entity on the Network.
C. Communications may not be encrypted so as to avoid security review.
D. Users should change passwords regularly and avoid easily guessed passwords. Users must only use their own personal password.
E. Users, including students, are required to notify their teacher, adult, or district representative whenever they become aware of information or messages that are dangerous, inappropriate, or make them feel uncomfortable.

Privacy

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

No student or staff user should have any expectation of privacy when using the district's network. The district provides the network system, email, and Internet access as a tool 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, shared files and electronic communications;
E. Email and other electronic communication;
F. Internet access; and
G. Any and all information transmitted or received in connection with network and email use.

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.

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 and instructional materials adoption procedures. Additionally, hardware and all applications, software, and operating systems must be currently supported by the manufacturer and 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.

Archive and Backup

Backup is made of all district email correspondence for purposes of public disclosure and disaster recovery. Staff, students and other critical district files are backed up on district servers regularly. The district complies with state law for specific records retention requirements.

Emerging Technologies

Emerging technologies, including artificial intelligence, are a rapidly advancing set of technologies for capturing data to detect patterns and automate decisions. These technologies are becoming increasingly ubiquitous, and it is essential for students to understand effective, ethical and safe use. Emerging technologies can enhance classroom learning, and implementation will be guided with proper training, ethical considerations, and responsible oversight. When utilizing emerging technologies to create or support the creation of texts or creative works, students and staff are expected to adhere to district policies and procedures, guidelines, the district's AUP, and any additional guidance provided by their classroom teacher.

Disciplinary Action

All users of the district's electronic resources are required to comply with the district's AUP and agree to abide by the provisions set forth in the district. Violation of any of the conditions of use explained in any of these documents could result in suspension or revocation of network access, and/or other electronic resources privileges. Additionally, violations of these documents could result in disciplinary action, outlined in procedure 3330 R3 Kennewick School District Discipline Matrix and staff guidelines.

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 people 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 staff member with questions about how to comply with this requirement should consult with the executive director of communications.

Adopted:	November 8, 1995
Amended:	August 22, 2001
Amended:	February 11, 2025