PROCEDURES

ELECTRONIC RESOURCES AND INTERNET SAFETY

K-20 Network Acceptable Use Guidelines/Internet Safety Requirements

These procedures are written to support the Electronic Resources Policy of the Board of Directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful, technologically-fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different from face-to-face interactions.

Network

The District 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 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.

Acceptable network use by District students and staff includes:

- Creation of files, digital projects, videos, webpages and podcasts using network resources in support of education and research;
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and webpages that support education and research;
- 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;
- Staff use of the network for incidental personal use in accordance with all District policies and procedures; and
- Connection of personal electronic devices (wired or wireless) when authorized, including portable devices with network capabilities to the District network after checking with the Director of Technology or his/her designee to confirm that the device 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 other District policies.

Unacceptable network use by District students and staff includes, but is not limited to:

- Personal gain, commercial solicitation and compensation of any kind;
- Actions that result in liability or cost incurred by the District;
- Downloading, installing and use of games, audio files, video files, games or other applications (including shareware or freeware) without permission or approval from the Director of Technology or his/her designee;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
- Storage of personal files on District computers or servers;
- Student use of a computer when a staff member is logged onto the computer;
- Support for or opposition to ballot measures, candidates and any other political activity;
- Unauthorized access to other District computers, networks and information systems;
- Cyber-bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Information posted, sent or stored online that could endanger others (e.g. bomb construction, drug manufacturing);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized devices to the District network. Any such device will be confiscated, and additional disciplinary action may be taken.
- 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 computer network or the Internet.

Accounts and Access

User accounts and the resources they can access will be customized for student grade levels and staff assignments. Different ages of students have different needs just as different job assignments have different technology needs. In places and situations where the only resource needed is logging onto a computer and using locally installed programs, staff and students can use shared accounts. However, when accessing wide varying Internet sites, individual accounts need to be created and used by students and staff.

Internet Safety

Personal Information and Inappropriate Content:

- Students and staff should not reveal personal information, including a home address and phone number, on websites, blogs, podcasts, videos, social networking sites, wikis, e-mail or as content on any other electronic medium;
- Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
- No student pictures or names can be published on any public class, school or District website unless the appropriate permission has been obtained according to District policy; and
- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

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.

- Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to District browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content);
- E-mail inconsistent with the educational and research mission of the District will be considered SPAM and blocked from entering District e-mail boxes;
- The District will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to District devices;
- 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; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

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 cyber-bullying awareness and response.

- Age appropriate materials will be made available for use across grade levels; and
- Training on online safety issues and materials implementation will be made available for administration, staff and families.

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 purview 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.

Network Security

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized District purposes. Students and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard user accounts:

- Change passwords according to District policy;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your user account password, keep it in a secure location;
- Do not store passwords in a file without encryption; and
- Lock the screen or log off if leaving the computer.

Student Data is Confidential

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

The District provides the network system, e-mail 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:

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and
- Any and all information transmitted or received in connection with network and e-mail 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. Access to student data will be restricted to staff that need access as dictated by their position and related tasks. Individuals working for other agencies such as ESD 113, Skokomish Indian Tribe and Squaxin Island Tribe that work with our students are granted access to student data pertaining to the students they are servicing. Before such access is granted there needs to be a Memorandum of Understanding between the outside agency and the District that outlines the limits of the access. Each individual from these outside agencies will sign a confidentiality statement that outlines the sensitive nature of the data they are allowed to access for and adhering to the confidentiality of the account they use to access this information.

Staff Accounts

District network accounts and e-mail accounts will be given to staff needing such access as part of their jobs. A minimal account that can be used for completion of online trainings will be given to staff that do not use a computer as part of their normal job functions. For District communications that are normally dispersed via

e-mail, it will be the responsibility of staff member's supervisors to make sure such information is posted for individuals that do not have e-mail accounts.

Records Retention

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

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 Director of Technology or his/her designee.

Disciplinary Action

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). Violation of any of the conditions of use explained in the Shelton School District Electronic Resources policy or in these procedures could be cause of disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Approved: 2/13/96
Revised: 5/25/04
Revised: 6/26/12
Revised: 4/10/18