Superintendent Procedure 2022SP
Electronic Resources/Use of the Internet

Approved by: *s/Dr. Brent C. Jones* Date: 5/13/24

Dr. Brent C. Jones, Superintendent

This procedure supports implementation of Board Policy No. 2022, Electronic Resources/Use of the Internet; Board Policy No. 2023, Digital Citizenship & Media Literacy; and related district policies and procedures. These policies and procedures are intended to promote positive and effective digital citizenship among students and staff.

Per Board Policy No. 2023 and RCW 28A.650.010, "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 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.

Annual Policy and Procedure Review

The district will annually review its policies and procedures on electronic resources, Internet safety, digital citizenship, and media literacy. In reviewing and amending the policy and procedures, per RCW 28A.650.045, the district will:

- Involve a representation of students, parents or guardians, teachers, teacher-librarians, other school employees, administrators, and community representatives with experience or expertise in digital citizenship, media literacy, and internet safety issues;
- Consider customizing the model policy and procedures on electronic resources and internet safety developed by the Washington state school directors' association;
- Consider existing school district resources; and
- Consider best practices, resources, and models for instruction in digital citizenship, internet safety, and media literacy, including methods to involve parents.

The Washington State School Directors' Association (WSSDA) checklist (2023F, Form—Checklist for Digital Citizenship, Media Literacy, Electronic Resources, and Internet Safety), developed pursuant to RCW 28A.650.040, provides a resource for the district to utilize and/or adapt for this annual review. This annual review may be conducted by or in collaboration with the Information Technology Advisory Committee.

Assignment of Student Devices

Each student is issued a district digital device (laptop or tablet). These district-provided devices may be used for in-classroom instruction and assessment and out-of-class assignments or remote learning, as necessary.

Students may be instructed by their schools or teachers to leave devices at school and/or to bring their device home at night, charge the device, and return to school with the device. Students are required to follow rules regarding acceptance and liability for the device and appropriate use of the device.

- **Responsibility for Loss or Damage**

Student devices and accessories will be provided by schools to their students at the beginning of the school year. The district expects students and their families to use their best efforts to protect their district-assigned device. Students and/or their parent(s) guardian(s) will receive a student device agreement for signature, and device usage and safety information.

Most students will need to return their SPS device and accessories at the end of the school year. Failure to return a device and accessories or damages may result in a fine or fee being levied as outlined in Board Policy No. 3520 and Superintendent Procedure No. 3520SP, Student Fees, Fines, or Charges.

- **Student Use of District Devices**

The district provides devices for students with the expectation that students will use the device for learning purposes. There are several reasons why a district device is required and a personal device is not suitable for instruction, assignments, and assessments. For example, with every K-12 student having a standard device, the district can maintain equity for all students and continuity of the educational and classroom environment for teachers. The district can maintain a safe and secure environment for all students and the network by ensuring security software is in place and up to date. District devices offer filtered Internet access whether the student is in the classroom or offsite, which offers greater protection from inappropriate materials or websites than unfiltered Internet access.

The district provides technical support and maintenance for district devices on a year-round basis including the ability to remotely connect to the device when needed. The district can provide a secure, reliable, and consistent testing environment for student assessments and update it as the vendor requires. The district can restrict software installations on district devices that are unrelated to the educational environment. The district can push updates and any necessary educational software to the device remotely or make it accessible to whomever needs it. The district cannot do the same for personal devices because of licensing restrictions.

- **School Distribution and Collection of Student Devices**

Student devices are distributed and collected by schools at the beginning and end of each school year. The Department of Technology Services (DoTS) will provide schools with a process for their distribution and collection of student devices. Student devices are reused for the coming year. Device loss and damage impacts the district's ability to ensure students have the best possible equipment.

Each school principal will designate a device collection coordinator to ensure devices are checked in at the conclusion of each school year. Principals will also designate a point of contact to support families with questions about lost devices and the collection of fines.

Student Personal Electronic Devices

District-assigned devices are used for classroom instruction, assignments, and assessments. Because a personal device cannot be managed or supported on the district network, the district does not allow students to opt-out of receiving a district device or to substitute their personal electronic device for their district-assigned device.

District devices have applications that are subject to licensing agreements, which do not permit installation on personal devices. Personally owned devices may not provide the same safeguards to help prevent inappropriate online conduct.

Students do not have an absolute right to possess or use personal electronic devices at school. School staff may further restrict the use of personal electronic devices on school grounds and during the school day absent an approved accommodation that addresses a specific and articulated student need (e.g. assistive technology). Students using personally owned devices may be asked to make the device available to the district in the event of an investigation involving inappropriate behavior (e.g. bullying, harassment, discrimination).

Personal devices may only be used on designated district guest networks. Seattle Public Schools is not responsible for support, maintenance, damage, or loss of any personal devices used in or on district facilities.

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 district network must support education or academic research and be consistent with the mission of the district. Additional district policies and procedures contain further requirements regarding the acceptable use of district technology and personal devices for staff and students.

All students will use electronic resources. At a family's request, per Board Policy No. 3540, students may be placed in a restricted access group that limits Internet access on district devices to curriculum and other classroom resources.

Acceptable network use by district students and staff may include:

A. Creation of files, camera images, 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 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. Staff use of the network for incidental personal use in accordance with all district policies and procedures; or
E. Personal electronic devices (wired or wireless) including portable devices with network capabilities may only be connected to designated district guest networks in accordance with applicable laws, district policies and procedures, the district network use agreement, and local school rules. Personal devices may not be connected to the non-guest district network.

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

A. Transmitting or accessing obscene, pornographic, graphically violent, or sexually inappropriate material or pictures for a non-educational purpose;
B. Using obscene, graphically violent, or sexually inappropriate language for a non-educational purpose;
C. Engaging in practices that may harm or destroy data on any system or on the network or disrupt the operation of the network;
D. Installing, storing, or distributing copyrighted software or materials in violation of copyright law;
E. Supporting or opposing a political candidate, an election campaign, or a ballot proposition, including a school levy (see *Guidelines for School Districts In Election Campaigns*, Public Disclosure Commission Interpretation No. 01-03)
F. Sharing computer authorization, including your password, with any person, except to an authorized network administrator or a minor student's parent or guardian;
G. Transmitting or accessing material that discriminates against, harasses, defames, or insults another person, which includes sending or receiving sexually explicit, racial, or gender inappropriate jokes or messages;
H. Using the network to violate district policies or procedures;
I. Encrypting communications to avoid district review;
J. Intentional and unauthorized access in another person's folders or work files;
K. Using the network for illegal activities (e.g., sale of drugs, bomb making, or computer trespass/hacking); or
L. Using district devices or the network for non-district approved commercial purposes.

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 their 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.

Internet Safety

- **Personal Information and Inappropriate Content**

A. Students and staff should minimize sharing 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;
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 according to district policies and procedures;
D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority; and
E. 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 in themselves. Every user must take responsibility for their use of the network and Internet and avoid objectionable material;
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. E-mail inconsistent with the educational and research mission of the district will be considered SPAM and may be blocked from entering district e-mail;
D. Staff 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
E. The district may monitor student use of the district network, including when accessed on students' personal or district-provided electronic devices.

- **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. Training on online safety issues and materials implementation will be made available for administration, staff, and students.
B. Age-appropriate materials will be made available for use across grade levels.
C. Each school will provide appropriate instruction for students on online safety each school year. Principals will provide direction to staff on which grade levels receive instruction, what materials are used, who will provide the instruction, and how many times instruction is provided in any one school year.

Network Security and Privacy

- **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 network user accounts:

A. Change passwords according to district policy;
B. Do not use another user's account;
C. Do not provide your passwords to others;
D. Do not insert passwords into e-mail or other communications;
E. If you write down your user account password, keep it in a secure location;
F. Do not use the "remember password" feature of Internet browsers; and
G. 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).

- **No Expectation of Privacy**

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:

A. The district network, including the guest network, when accessed by personal electronic devices and SPS-issued devices;
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 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 writings prepared, owned, used, or retained by the district are subject to the public records disclosure laws of the State of Washington.

Disciplinary Action

All users of the district's electronic resources are required to comply with the district's policies and procedures (and agree to abide by the provisions set forth in the district's network use agreement). Violation of any of the conditions of use explained in the network use agreement, or relevant policies and procedures could be cause for disciplinary action, including exclusion from school and suspension or revocation of network and computer access privileges.

Accessibility of Electronic Resources

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 webmaster (webmaster@seattleschools.org).

Copyright and Ownership of Work

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.

Board Policy No. 2025 and Superintendent Procedure 2025SP, Copyright: Acquisition and Compliance, provide additional requirements for the use of copyrighted material and ownership of work.

Approved: September 2012
Revised: May 2024
Cross Reference: Policy Nos. 2021; 2022; 2023; 2025; 2080; 3207; 3208; 3225; 3231; 3520; 3540; 4020; 4040; 4070; 5252; 5253; 6501; *Basic Rules of Seattle Public Schools*