Superintendent Procedure 2022SP

Electronic Resources/Use of the Internet

Approved by: *s/José Banda* Date: 9/27/12

Dr. José Banda, Superintendent

Electronic Resources

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.

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 e-readers) 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. 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 network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students and staff 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 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. Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the district network is not allowed. Personal electronic devices 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.

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;
F. Sharing computer authorization, including your password, with any person, except to an authorized network administrator.
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;
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 “hacking”); and
L. Using District computers or the network for non-District approved commercial purposes, including a private or personal business or consulting practice

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.

Internet Safety

Personal Information and Inappropriate Content:

A. Students and staff 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 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 policy; and
D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

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 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. E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
D. 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.

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. Each school will provide appropriate instruction for students on online safety each school year. Principals have final say 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
B. Age appropriate materials will be made available for use across grade levels.
C. Library Services will provide support and training for librarians to conduct online safety instruction.

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 network;
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 documents are subject to the public records disclosure laws of the State of Washington.

Archive and Backup

Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery for 7 years from the date of creation. Barring power outage or intermittent technical issues, staff and student files are backed up on district servers regularly. Refer to the district retention policy and the district's Archives department for specific records retention requirements.

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 (district's user agreement), Electronic Resources 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.

Approved: September 2012
Revised:
Cross Reference: Policy No. 2022, Policy No. 2025