

## **Instruction**

### **Electronic Resources and Internet Safety Procedures**

#### **Acceptable Use Guidelines/Internet Safety Requirements**

These procedures are written to support the Electronic Resource and Internet Safety Policy of the district and are 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, including digital and media literacy, ethics, etiquette, and security. The term also includes the ability to access, analyze, evaluate, develop, produce, and interpret media, as well as internet safety and cyberbullying prevention and response. 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.

#### **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 used for school activities (on or off school premises) are subject to the same procedures as district provided services.

#### **Network**

The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (such as blogs, websites, collaboration software, social networking sites, wikis, etc.). This also applies to district provided devices (such as laptops, tablets, and hot spots) for student's use outside of the school premises.

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

#### **General Requirements**

1. Use of the district network has been established for specific and directed educational purposes and school-related business and operations. The term "educational purpose" includes classroom activities, career development, and research.
2. The district restricts the use of district network resources to authorized users, and equipment. The district network has not been established as a public forum. The district

has the right to place reasonable restrictions on the material accessed or posted through the district network.

- a. District resources are provided “as is” for personal devices.
  - b. The district does not warrant personal devices that use district resources from damage, or loss of data, introduction of malicious software, or corruption of software.
3. Users of the district network must first agree to the appropriate Acceptable Use Agreement. The user’s acceptance of the electronic version of the Agreement signifies the user’s acknowledgement and agreement to abide by the Acceptable Use Agreement. Users may be required to agree to the respective Acceptable Use Agreement more than once each year. A hard copy of the Acceptable Use Agreement is located in the student handbook and is available at the school or on the district website in Policy and Procedure Section 2022.
  4. Individuals with district network user accounts are responsible for all activity conducted on or through the district network via their user account. Each district network user account is to be used only by the authorized holder of the account for the authorized purpose(s). The district will provide ways for users to maintain required privacy of information, such as through screen locking or similar processes.
  5. The district reserves the right to prioritize use of, and access to the system. The district may limit or exclude users’ ability to access parts or functions of the district network and other resources that can be accessed through the district network.
  6. Any use of the district network must comply with state and federal law and other district policies, procedures, and guidelines regarding computer and internet use.

### **Unacceptable Use**

Doing or assisting any of the following activities via the district network is prohibited:

1. Engaging in any activity that violates local, state, and/or federal laws.
2. Interfering with or disrupting other district network users, services or equipment. This includes distribution of unsolicited advertising, propagation of malicious code and viruses, denial of service types of attacks, and/or using the district network to attempt or make unauthorized entry into any other resource accessible via the district network.
3. Making unauthorized copies of or changes to files or other data not their own.
4. Using the district network to access confidential student, employee, or other information that the user is not specifically authorized to access.

5. Vandalizing, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the integrity of the district network or any computer-based information and/or information resources accessible via the district network. In this context, “vandalism” means to harm, materially inhibit, or destroy any such items, or to attempt to do any of those things.
6. Using the district network in a manner that violates the district’s prohibition against harassment, intimidation, and bullying in Policy 3207 and Procedure 3207P.
7. Using the district network for personal or private gain, personal business, commercial solicitation, or personal compensation of any kind.
8. Supporting or opposing political candidates, ballot measures, or any other political activity.
9. Using the district network to access, upload, post, store, transmit, publish, or display harassing, intimidating, bullying, defamatory, libelous, scandalous, intentionally inaccurate, discriminatory, abusive, profane, sexually oriented, or threatening content of any form, including materials, language, photographs, videos, or messages, either public or private.
10. Downloading, installing or using unlicensed or unauthorized software, files, or other applications on the District network or devices or on personal devices while connected to the district network.
11. Engaging in plagiarism or violation of copyright laws or other intellectual property rights.

### **District Rights**

The Snohomish School District reserves the right to:

1. Monitor and manage all activity on the district network.
2. Notify parents of their students’ activity on the district network, subject to any restrictions of applicable law.
3. Determine acceptable use standards for the district network and enforce disciplinary consequences for any breach of Procedure 2022P. Disciplinary action, if any, for students, staff, and other users will be consistent with the district’s policies, procedures, and standard practices. Consequences may include revocation of access privileges, suspension of access to the district network, computers, or other devices, other school disciplinary action, and/or appropriate legal action. Specific disciplinary measures will be determined on a case- by-case basis.
4. Prohibit or prevent unauthorized devices from accessing the district network.

### **No Expectation of Privacy**

The district reserves the right to monitor, inspect, copy, review, and store, without prior notice, information about the content of usage of:

- A. The district network, including when accessed on personal electronic devices and on devices provided by the district, including laptops, netbooks, and tablets;
- B. User files and disk space utilization;
- C. Applications and bandwidth utilization;
- D. User document files, folders, and electronic communications;
- E. Email;
- F. Internet access; and
- G. Any and all information transmitted or received in connection with network and email.

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 or records are subject to the public records disclosure laws of the State of Washington.

### **District Limitation of Liability**

The district makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the district network will be error-free or without defect. The district will not be responsible for any damage users may suffer, including theft or loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the district network. The district will not be responsible for financial obligations arising from unauthorized use of the district network. The district will not be responsible for any damage to personal computing devices that intentionally or unintentionally access the District network.

### **District Network Code of Conduct**

Individuals who use the district network or resources must abide by the following Code of Conduct:

1. I will protect my logon and personal information from others. I will never give out personal information via the district network, such as my home addresses/phone numbers, credit card number, Social Security number or drivers' license number.
2. I will respect the privacy of other users. I will not use others' passwords.
3. I will always use the internet responsibly. I will not use the district network to access pornographic or otherwise inappropriate material. I will immediately inform my teachers,

parents or a district administrator if I encounter any information that is inappropriate, discriminatory, harassing, hateful or obscene.

4. Unless I have specific permission from the district, I will make sure that anything I publish using the district network is done in my name only, and not on behalf of the district. If I upload content using the district network, I will make sure that I have the authority to make it available to others.
5. I will follow appropriate online behavior, including interacting with other individuals on shared documents, social networking websites, and in chat rooms,
  - a. I will not access, send, or post inappropriate, hateful, discriminatory, harassing, or obscene messages.
  - b. I will not develop or distribute programs or messages that harass other users or infiltrate a computer. I will not “hack” the district network (e.g., by introducing or transmitting viruses, worms, “chain letters,” global mailings, etc.).
  - c. I will not modify or copy files/data of other users without their consent.
  - d. I will not click on links embedded in e-mails from unknown senders, or even in emails that appear to be from someone I know but that are unusual or suspicious to me.
6. I will obey copyright and other intellectual property laws. I will not bind the district to any license or other contract, including any click-to-agree license or other agreement, unless I have express authority from the district to do so.
7. I will follow any district instructions regarding maintenance or care of the district network. I will not delete or add peripheral equipment to the district network without permission. I will not destroy, modify or abuse the district network hardware or software in any way. This includes:
  - a. Installing or running any program I am not authorized to access.
  - b. Reconfiguring system or software settings unless instructed to by district technology staff.
8. I will not use the district network for commercial or political purposes.
9. I understand that the district may restrict or remove my user account if it is determined that I have engaged in unauthorized activity or am violating any part of Procedure 2022P, including this Code of Conduct.

Adoption Date: October 25, 1995

Revision Dates: March 25, 1998  
September 12, 2001  
August 12, 2009  
August 28, 2011  
January 28, 2015  
May 25, 2016  
August 22, 2018  
August 31, 2020