

#### **K-20 Network Acceptable Use Guidelines/Internet Safety Requirements**

These procedures are written to support the Electronic Resources Policy of the Board 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 the 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 computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, 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.

1. Annually, It is assumed that parents grant their child the right to access the network and has a desire to have their child use the Internet as an educational resource unless the parent signs and returns the opt out form that is included as part of the annual enrollment form.
2. Annually, students will receive grade level instruction on digital citizenship and Internet Safety educating them about appropriate online behavior, using personal portable devices at school, interacting with other individuals on social networking websites and cyber-bullying awareness and response.
3. Annually, all staff must sign an Acceptable Use and Internet Safety Agreement or take an online Acceptable Use and Internet Safety course before access will be granted to the Network.
4. Use of the computer network and Internet is a privilege, not a right. A user who violates this agreement shall, at a minimum, have his or her access to the network temporarily terminated. The District may also take other disciplinary actions as appropriate.

Acceptable network use by District students and staff includes:

1. Creation of files, digital projects, videos, web pages and podcasts using network resources in support of educational research;
2. Participation in blogs, wikis, bulletin boards, social networking sites and groups, and the creation of content for podcasts, e-mail and web pages that support educational research;
3. 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;
4. Student and Staff use of the network for incidental personal use in accordance with all District policies and procedures;
5. Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the District network after receiving appropriate approval. Students will only use personal electronic devices on the District's network at the discretion and approval of their teacher, school building staff and/or administration. District staff will check with their supervisors once at the beginning of each school year. Connection of any personal electronic device to the District network by any person is subject to all procedures in this document.

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

1. Personal gain, commercial solicitation and compensation of any kind ;
2. Actions that result in liability or cost incurred by the District;
3. Downloading, installing and use of games, audio files, video files, or other applications for anything other than in the support of educational research;
4. Support or opposition for ballot measures, candidates and any other political activity;
5. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
6. Unauthorized access to other District computers, networks and information systems;
7. Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
8. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);

9. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
10. Attaching unauthorized devices to the District network.  
Any such device will be confiscated and additional disciplinary action may be taken.

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 its 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:

1. 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;
2. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
3. 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
4. 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 and/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.

1. Filtering software is not 100% 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 or her use of the network and Internet and avoid objectionable sites;

2. Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to District browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;
3. E-mail inconsistent with the educational and research mission of the District will be considered SPAM and blocked from entering District e-mail boxes;
4. 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 computers;
5. 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
6. 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 cyberbullying awareness and response.

1. Age appropriate materials will be made available for use across grade levels.
2. 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 are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

### **Network Security and Privacy**

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:

1. Change passwords according to District policy;
2. Do not use another user's account;
3. Do not insert passwords into e-mail or other communications;
4. If you write down your user account password, keep it in a secure location;
5. Do not store passwords in a file without encryption;
6. Do not use the "remember password" feature of Internet browsers; and
7. 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:

1. The network;
2. User files and disk space utilization;
3. User applications and bandwidth utilization;
4. User document files, folders and electronic communications;
5. E-mail;
6. Internet access; and
7. Any and all information transmitted or received in connection with Network and e-mail use.

Student or staff users should not 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 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 on a regular basis. Refer to the District retention policy 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 online network user agreement training, Internet safety training, student handbook, Electronic Resources Policy and/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.

## **Use of Social Media, Web-based or Internet Tools**

Online communication is critical to our students' learning of 21st Century Skills. Social media, Web-based or Internet tools such as blogs, wikis, social networks, podcasts, email, or other Internet tools offer an authentic, real-world vehicle for student expression. Examples of social media include, but are not limited to, Facebook, Twitter, YouTube, Google+, Instagram, Linked In, and Flickr. Our primary responsibility to students is their safety. Hence, the District holds those staff and students, using these tools to the same acceptable use, terms of agreement, standards and expectations and must follow all established Internet safety guidelines. Furthermore, if you are going to use these tools in your official capacity the District reserves the right to monitor appropriate behavior and adherence to instructional guidelines. Anything deemed to be inappropriate will be subject to deletion.

Building principals will identify staff and students who request the use of these tools to ensure they are aware of and understand the benefits, risks and personal responsibility of using these tools is understood. To that end, building principals will ensure annually, all staff and students have an adequate opportunity to access the Internet safety instruction required by the District and communicate with parents regarding its school's use of these tools and the Internet safety measures in place.

### **Internet Tools Terms and Conditions:**

1. Students and staff using blogs, wikis, social networks, podcasts, email, new media or other web tools are expected to act safely by keeping all personal information out of their posts.
2. Students and staff using such tools agree to not share their user name or password with anyone besides their teachers and parents and treat blog spaces as classroom spaces. Speech that is inappropriate for class is also inappropriate for a blog.
3. All terms of use for electronic resources also apply to these tools and therefore the same conditions of use and misuse apply.

Students and staff who do not abide by these terms and conditions may be disciplined and lose their opportunity to take part in the project and/or be subject to consequences appropriate to misuse.

## **1. Guidance Regarding Professional Social Media Sites**

- a. All District employees should treat professional social media space and communication like a classroom and/or a professional workplace. The same standards expected in District professional settings are expected on professional social media sites. If a particular type of behavior is inappropriate in the classroom or a professional workplace, then that behavior is also inappropriate on the professional social media site;
- b. All District employees should exercise caution, sound judgment, and common sense when using professional social media sites;
- c. All District employees should use privacy settings to control access to their professional social media sites to ensure that professional social media communications only reach the employees' intended audience. However, employees should be aware that there are limitations to privacy settings. Private communication published on the internet can easily become public. Furthermore, social media sites can change their current default privacy settings and other functions. As a result, employees have an individualized responsibility to understand the rules of the social media site being utilized;
- d. Professional social media communication should be in compliance with existing District policies and applicable federal and state laws, including, but not limited to, prohibitions on the disclosure of confidential information and prohibitions on the use of harassing, obscene, discriminatory, defamatory or threatening language;
- e. No personally identifiable student information may be posted by District employees on professional social media sites, including student photographs, without the consent of the students' parents; and

## **2. Press Inquiries**

Any press inquiries received via professional social media sites should be promptly referred to the District administrative office.

## **E. Personal Social Media Use**

### **1. Communication with Students**

In order to maintain a professional and appropriate relationship with students, District employees should not communicate<sup>1</sup> with students who are currently enrolled in District schools on personal social media sites. This provision is subject to the following exceptions: (a) communication with relatives and (b) if an emergency situation requires such communication, in which case the District employee should notify his/her supervisor of the contact as soon as possible.

### **2. Guidance Regarding Personal Social Media Sites**

District employees should exercise caution and common sense when using personal social media sites:

- a. As a recommended practice, District employees are encouraged to use appropriate privacy settings to control access to their personal social media sites. However, be aware that there are limitations to privacy settings. Private communication published on the internet can easily become public. Furthermore, social media sites can change their current default privacy settings and other functions. As a result, employees have an individualized responsibility to understand the rules of the social media site being utilized;
- b. District employees should not “tag” photos of other District employees, District volunteers, District contractors or District vendors without the prior permission of the individuals being tagged;
- c. Personal social media use, including off-hours use, has the potential to result in disruption at school and/or the workplace, and can be in violation of District policies and federal and/or state law;
- d. The posting or disclosure of personally identifiable student information or confidential information via personal social media sites, in violation of these Guidelines is prohibited; and

---

<sup>1</sup> Examples of such communications include, but are not limited to, “friending,” “following,” “commenting,” “liking,” and posting messages.



- e. District employees should not use the District's logo in any postings and should not link to the District's website or post District material on any personal social media sites without the written permission of a District administrator.

### **Use of Personal Mobile Devices**

Peninsula School District recognizes that personal mobile phones and digital devices are now an integral part of our community, culture and way of life. It is also recognized that these personal devices will play a significant part in the education of the 21<sup>st</sup> century student. Therefore, in accordance with all District policies and procedures, students, staff, parents and our community may use personal electronic devices (e.g. laptops, mobile devices and e-readers) while on District property to further the educational and research mission of the District. District and school administration will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day.

### **General Conditions for Personal Mobile Device Use**

1. The term personal mobile device in this policy denotes mobile phones, laptops, notebooks, iPod touches, tablets such as the iPad or Android OS device or any similar mobile device that can access the Peninsula School District network and/or the Internet.
2. All provisions, guidelines and procedures in Peninsula School District Policy 2022 apply to all personal portable devices connected to the District's network whether or not permission was granted.
3. Parents or guardians must grant permission before their students can bring personal mobile devices to school whether the device will be used for emergency, personal and/or educational use.
4. It is assumed students who bring any personal portable device on District property have been granted permission to do so from their parents or guardians and agree to follow the acceptable use procedures for personal mobile devices.
5. Parents or guardians not granting permission for their student to use personal mobile devices on District property must notify the school in writing to the Principal or their designee.
6. The acceptable use procedures for mobile devices also apply to students during school excursions, camps and extra-curricular activities.

7. The use of a personal mobile device by staff, students, parents or community members on District property must adhere to the District's acceptable use procedures for mobile devices as well as all provisions of the Electronic Resources Policy and Procedures.
8. Failure to follow these acceptable use procedures may subject staff or students to the District's Code of Conduct and may result in disciplinary action.

### **Acceptable Use of Personal Mobile Devices by Students**

1. Staff and students will take complete responsibility for their personal mobile devices while at school.
2. Staff and students will keep the mobile device secure and locked away when not in use and never leave it in any open area unattended.
3. Each school will determine specific acceptable use of a personal mobile device.
4. School staff will determine the appropriate use of personal mobile devices for students during instructional time in the classroom.
5. School staff has the right to allow or disallow the use of personal mobile devices during instructional time as appropriate.
6. School staff has the right to determine whether personal mobile devices are stored out of sight or placed on the student's desk in plain sight.
7. Student's personal mobile devices with Internet access capabilities are expected to access the Internet through the school's filtered network while on school property.
8. Student's personal mobile devices will never be used in any manner or place that is disruptive in a classroom, school, or while participating in any other activity in the District.
9. Using personal mobile phones or devices to bully and threaten other students is unacceptable and will not be tolerated.
10. Pictures and videos must not be taken of students, teacher or other individuals without their permission.

## **District's Responsibilities to Support Use of Personal Mobile Devices**

1. The District will provide a safe, monitored and filtered wireless network according to the Children's Internet Protection Act for students to use with their personal mobile devices.
2. If the District has reasonable cause to believe the student has violated the AUPMD, authorized personnel may search a student's mobile device.
3. Any use of the personal mobile device that is deemed a criminal offense, will be dealt with as such by the District.
4. The District may remove the user's access to the network and suspend the right to use the personal mobile device on District property if it is determined that the user is engaged in unauthorized or illegal activity or is violating the Electronic Resources policy and procedures.
5. The district assumes no liability or responsibility for students that misuse mobile devices while on school property.
6. District staff will reasonably monitor and supervise students as they use personal mobile devices while at school.
7. The District will educate students in identifying, promoting, and encouraging best practices, good digital citizenship and Internet safety specifically for personal mobile devices.
8. The District accepts no financial responsibility for damage, loss, theft or costs associated with the use of the personal mobile devices while at school.

## **Email and Internet Communications Etiquette and Protocols**

Email and other Internet communication tools such as blogs, wikis and social networks are provided by the Peninsula District for your professional and educational use. These systems are not be used for extensive or ongoing personal communications. Internet communications are most effective when it has clarity, conciseness, and courtesy.

**Date: 11/2009**  
**Updated: 08/2011**  
**Revised: 06/2012**  
**Revised: 07/2013**  
**Revised: 11/2015**