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.

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 after checking with Technology Director 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.

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

a. Personal gain, commercial solicitation and compensation of any kind;
b. Actions that result in liability or cost incurred by the district;

c. Downloading, installing and use of games, audio files, video files, games or other applications (including shareware or freeware) without permission or approval from the Technology Director;
d. Support for or opposition to ballot measures, candidates and any other political activity;
e. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
f. Unauthorized access to other district computers, networks and information systems;
g. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
h. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
i. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; or
j. 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 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;
e. 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
f. 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.

a. Age appropriate materials will be made available for use across grade levels.
b. 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 Fair Use Doctrine 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 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:

a. Change passwords according to district policy;
b. Do not use another user's account;
c. Do not insert passwords into e-mail or other communications;
d. If you write down your user account password, keep it in a secure location;
e. Do not store passwords in a file without encryption;
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. 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.

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.

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

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 and volunteers 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 and volunteers should exercise caution, sound judgment, and common sense when using professional social media sites;

c. All District employees and volunteers should use privacy settings to control access to their professional social media sites to ensure that professional social media communications only reach the employees' and volunteers' intended audience. However, employees and volunteers 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 and volunteers 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;

No personally identifiable student information may be posted by District employees and volunteers on professional social media sites, including student photographs, without the consent of the students' parents; and

2. Press Inquiries

Any media inquiries received via professional social media sites should be promptly referred to the District's Public Information Officer.

Personal Social Media Use

1. **Communication with Students**

In order to maintain a professional and appropriate relationship with students, District employees and volunteers should not communicate[1] 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 employees and volunteers should notify his/her supervisor of the contact as soon as possible.

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

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

a. As a recommended practice, District employees and volunteers 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 and volunteers have an individualized responsibility to understand the rules of the social media site being utilized;

b. District employees and volunteers shall 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

e. District employees and volunteers shall 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.

---

[1] *Examples of such communications include, but are not limited to, "friending," "following," "commenting," "liking," and posting messages.*

Use of Personal Mobile Devices

Bremerton 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 21st 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 Bremerton School District network and/or the Internet.

2. All provisions, guidelines and procedures in Bremerton 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 (AUPMD) 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, teachers 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 Bremerton School 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.

Bremerton School District

January 2017