Responsible Use of 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.

Policy 2022 and its procedures apply to all staff, students, and guest users of the school district's network, electronic devices, and resources.

Use of Personal Electronic Devices

In accordance with all district policies and procedures, students and staff may use personal electronic devices such as, but not limited to, laptops, mobile devices, cell phones, and e-readers to promote student learning and to further the educational and research mission of the district. The use of personally owned devices at school by staff and students is voluntary and a privilege, and subject to all school district policies and procedures. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during any school-related activity.

The district assumes no liability or responsibility for any act of a staff, student or guest user that is inconsistent with school district policies and procedures. Any individual who brings personally owned devices onto school property is solely responsible for that equipment.

If the District has reasonable cause to believe a staff member or student has violated school district policies or procedures authorized personnel may confiscate and search a staff, student's or guest user's mobile device in accordance with school district policies and procedures for privacy, and search and seizure.

Network Use

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. Policies and procedures related to use of the district network resources includes access through district-owned and personally-owned computing devices. The district reserves the right to prioritize the use of, and access to, the network.

Staff, students and parents/guardians, and guest users may be asked to sign a network use agreement before access to the district network and electronic resources is granted. The signed agreement will remain in force unless the parent/guardian notifies the district to revoke his/her child's privilege to access network resources or the user has violated district policies or

procedures. Violations may result in suspension or termination of network privileges and be subject to other disciplinary action according to district policies.

All network use is intended to support education and research and be consistent with the mission of the district. Guest users may be granted access to the district network and electronic resources by the Director of Technology or designee. Guest users are subject to all school district policies and procedures.

Connection of any personal electronic device to the district network by any person is voluntary and a privilege, and subject to all school district policies and procedures.

Responsible and acceptable use of technology by district network users includes:

A. Creation of files, digital projects, videos, web pages and podcasts 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. The online publication of original educational material, curriculum related materials, and student work. Parental and student permission must be received in writing electronically or in hard copy before publishing student work. Sources outside the classroom or school must be cited appropriately;
D. Connection of personal electronic devices, wired or wireless, including Internet-capable portable devices to the district network upon permission from the Director of Technology or designee to confirm that the device is equipped with up-to-date anti-virus software, compatible network card, and is configured properly. Connection of any personal electronic device is subject to all district policies and procedures. Permission may be granted in an electronic format as part of the network login process; or
E. Staff use of the network for incidental personal use in accordance with all district policies and procedures.

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) for non-educational purposes unless hard-copy or electronic written permission has been received from the Director of Technology or designee;
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 or 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;
J. Intentionally searching for inappropriate material (e.g. bomb construction, pornography, sexually explicit material); or
K. Attaching or connecting unauthorized devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken according to district policies and procedures.

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 the user's own negligence or any other errors, omissions, or breach of these procedures. 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. Students or staff encountering dangerous or inappropriate information or messages are obligated to notify the appropriate school authority immediately.

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 and resources will be made available for use across grade levels.
B. Training in or information about online safety issues and materials will be made available for staff, students, and families.

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 made at the school district's sole discretion.

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 such as, but not limited to, proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication or distribution 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 by reasonably monitoring and supervising students as they use the Internet and electronic resources at school;
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.
F. The district will review its Internet filter categories at least once a year to ensure the Internet filtering software category filters are set appropriately in accordance with federal, state, and district policies including the Childrens' Internet Protection Act.
G. The district will provide methods for staff and students to request a review for access to a site or filtering category that may have been mis-categorized or is blocked by the district's Internet filtering software. The content on the requested website or in the category must be consistent with and for the purpose of education and research in support of the district's mission. Information for requests to review a website or categorization can be located on the BISD website under Programs & Services/Technology/Content Filtering.

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, staff, or guest user should have any expectation of privacy when using the district's network or electronic resources. 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. All district staff e-mail correspondence is archived for purposes of public disclosure and disaster recovery. The district will archive based on its records retention policy according to 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 district user agreements. Violation of any of the conditions of use explained in Policy 2022 and related district policies, in these procedures, or related user agreements could be cause for disciplinary action. Consequences for inappropriate behavior could include limited network access, suspension or revocation of network and computer privileges or other disciplinary action in accordance with school district policies and procedures.