Electronic Resources ~~Electronic Information System (Networks)~~

~~Acceptable Use Guidelines~~

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 than 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.

Acceptable network use by district students and staff includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research;
- 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;
- 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;
- Staff use of the network for incidental personal use in accordance with all District policies and guidelines;
- Connection of staff personal laptops to the district network after checking with (*insert title of position, i.e., technology director, IT director, assistant superintendent*) to confirm that the laptop 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 guidelines in this document.

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

- Personal gain, commercial solicitation and compensation of any kind;
- Liability or cost incurred by the district;
- Downloading, installation and use of games, audio files, video files or other applications (including shareware or freeware) without permission or approval from the (*insert title of position*);
- Support or opposition for ballot measures, candidates and any other political activity;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;

- Unauthorized access to other district computers, networks and information systems;
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and destroyed.

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.

~~1. All use of the system must be in support of education and research and consistent with the mission of the district. District reserves the right to prioritize use and access to the system.~~

~~2. Any use of the system must be in conformity to state and federal law, network provider policies and licenses, and district policy. Use of the system for commercial solicitation is prohibited. Use of the system for charitable purposes must be approved in advance by the superintendent or designee.~~

~~3. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.~~

~~4. No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified or abused in any way.~~

~~5. Malicious use of the system to develop programs that harass other users or gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited.~~

~~6. Users are responsible for the appropriateness and content of material they transmit or publish on the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited.~~

~~7. Use of the system to access, store or distribute obscene or pornographic material is prohibited.~~

~~8. Subscriptions to mailing lists, bulletin boards, chat groups and commercial on-line services and other information services must be pre-approved by the superintendent or designee.~~

Internet Safety

Personal Information and Inappropriate Content:

- Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, wikis, e-mail or as content on any other electronic medium.
- Students and staff should not reveal personal information about another individual on any electronic medium.
- No student pictures or names can be published on any class, school or District web site unless the appropriate permission has been verified according to district policy.
- 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.

- 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;
- 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;
- E-mail inconsistent with the educational and research mission of the District will be considered SPAM and blocked from entering District e-mail boxes;
- 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;
- 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
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

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.

All student work is copyrighted. Permission to publish any student work requires permission from the parent or guardian.

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:

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

- The network;
- User files and disk space utilization;
- User applications and bandwidth utilization;
- User document files, folders and electronic communications;
- E-mail;
- Internet access; and
- 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 nightly – Monday through Friday. 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.

~~Security~~

~~9. System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.~~

~~10. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system, or attempt to gain unauthorized access to the system.~~

~~11. Communications may not be encrypted so as to avoid security review.~~

~~12. Users should change passwords regularly and avoid easily guessed passwords.~~

~~Personal Security~~

~~13. Personal Information such as addresses and telephone numbers should remain confidential when communicating on the system. Students shall never reveal such information without permission from their teacher or other adult.~~

~~14. Students shall never make appointments to meet people in person that they have contacted on the system without district and parent permission.~~

~~15. Students shall notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate or make them feel uncomfortable.~~

~~Copyright~~

~~16. The unauthorized installation, use, storage or distribution of copyrighted software or materials on district computers is prohibited.~~

~~General Use~~

~~17. Diligent effort must be made to conserve system resources. For example, users should frequently delete E-mail and unused files.~~

~~18. No person shall have access to the system without having received appropriate training, and a signed Individual User Release Form must be on file with the district. Students under the age of 18 must have the approval of a parent or guardian.~~

~~19. Nothing in these regulations is intended to preclude the supervised use of the system while under the direction of a teacher or other approved user acting in conformity with district policy and procedure.~~

~~From time to time, the district will make a determination on whether specific uses of the system are consistent with the regulations stated above. Under prescribed circumstances non-student or~~

~~staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district. For security and administrative purposes the district reserves the right for authorized personnel to review system use and file content. The district reserves the right to remove a user account on the system to prevent further unauthorized activity.~~

~~Violation of any of the conditions of use may be cause for disciplinary action.~~

Revision Date: 10/27/08