POLICY NO. 1800
Adopted: 6-12-96
Revised: 8-8-01
Revised: 5-23-12

ELECTRONIC RESOURCES

POLICY:

The Board of Directors recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The Board also believes that students need to be proficient and safe users of information, media, and technology to succeed in a digital world.

Therefore, the District will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the District's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings use these tools. The District's technology will enable educators and students to communicate, learn, share, collaborate, and create; to think and solve problems; to manage their work; and to take ownership of their lives.

To help ensure student safety and citizenship in online activities, all students will be educated about appropriate behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber-bullying awareness and response.

The Superintendent or designee will create strong electronic educational systems that support innovative teaching and learning, to provide appropriate staff development opportunities, and to develop procedures to support this policy.

Cross References:

Board Policies -

1325	Public Access to District Records
1430	Notification of Threats of Violence or Harm
4800	Sexual Harassment of Personnel
4900	Maintaining Professional Staff/Student Boundaries
5100	Students Rights and Responsibilities
5100.1	Secondary Discipline
5100.2	Elementary Discipline
5200	Protection of the Rights and Privacy of parents and Students
5230	Student Records
5500	Sexual Harassment of Students
5580	Prohibition of Harassment, Intimidation and Bullying
6008	Instructional Materials

Legal References:

18 USC §§ 2510-2522	Electronic Communication Privacy Act
Pub. L. No. 110-385	Protecting Children in the 21st Century Act

Management Resources:

Policy News, February 2012	
Policy News, June 2008	Electronic Resources
Policy News, June 2001	Congress Requires Internet Blocking at School
Policy News, August 1998	Permission required to review e-mail

POLICY NO. 1800
Adopted: 6-12-96
Revised: 8-8-01
Revised: 2-23-11
Revised: 5-23-12

ELECTRONIC RESOURCES

PROCEDURES:

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 STAFF AND STUDENTS

- 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 personal electronic devices (wired or wireless) including portable devices with network capabilities to the district network after checking with the District's Technology Director or designee to confirm that the device is equipped with up-to-date virus software, a 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 STAFF AND STUDENTS

- Personal gain, commercial solicitation, and compensation of any kind;
- Actions that result in 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 Superintendent or designee;
- 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;
- Cyber-bullying, 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;
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and additional disciplinary action may be taken;
- Intentionally wasting limited resources.

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

- 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;
- Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
- No student pictures or names can be published on any public class, school, or district web site unless the appropriate permission has been obtained according to district policy; and
- 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÷ (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);
- 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 devices;
- 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.

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 cyber-bullying awareness and response.

- Age appropriate materials will be made available for use across grade levels.
- 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

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. Communications may not be encrypted so as to avoid a security review. 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's 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.

Dear Parents:

Your child has the opportunity to receive an electronic network account or access and needs your permission to do so. Among other advantages, your child will be able to communicate with other schools, colleges, organizations, and individuals around the world through Internet and other electronic information systems and networks. Internet is a system which links smaller computer networks, creating a large and diverse network. Internet allows your child, through electronic mail (e-mail) and other means to reach out to many other people to share information, learn concepts, and research subjects. These are significant learning opportunities to prepare your child for the future.

With this educational opportunity also comes responsibility. It is important that you and your child read the enclosed Informed Consent Form, school district procedures and other material, and discuss it together. When your child is given an account and password to use on the computer, it is extremely important that the rules are followed. Inappropriate use will result in the loss of the privilege to use this educational tool and other disciplinary action if appropriate. Parents, remember that you are legally responsible for your child's actions.

Please stress to your child the importance of using only his or her account password and of keeping it a secret from other students. Your child should never let anyone else use his/her password to access the network. Your child is responsible for any activity that happens in his/her account.

We have established procedures and rules regulating the materials that students may search for on the network, but please be aware that there is unacceptable and controversial material and communications on the Internet that your child could access. It is not possible for us to always provide direct supervision of all students. We cannot filter material posted on network-connected computers all over the world. We encourage you to consider the potential of your child being exposed to inappropriate material in your decision of whether or not to sign the Informed Consent Form.

If you have any questions, please contact me at telephone number. If you want your child to have the opportunity to receive and electronic network account or access, please return a signed Informed Consent Form to us as soon as possible.

Sincerely,

User access request forms are available on the district's website.