WASHINGTON STATE SCHOOL FOR THE BLIND

POLICY: Date: August 18, 2003
Updated: May 8, 2012
Updated: January 24, 2013
Updated: September 20, 2019

SUBJECT: Acceptable Use of Electronic Resources

Prepared by: Danya Borowski, IS Manager

Approved by: _____
Scott McCallum, Superintendent

Instruction
Washington State School for the Blind's (WSSB) intentions for publishing an Acceptable Use of Electronics Resources Policy are not to impose restrictions that are contrary to WSSB established culture of openness, trust and integrity. WSSB in committed to protecting its students, employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

The Washington State School for the Blind recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The Superintendent along with the school's ex-officio board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, the Washington State School for the Blind 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 school's goal to provide students with rich and ample opportunities to use technology for important purposes just as individuals in workplaces and other real-life settings. The school'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 and Board of Trustees will direct the appropriate designee to 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.

This policy applies to employees, contractors, consultants, temporaries and other workers at WSSB including all personnel affiliated with third parties as well as students.

Cross References

Policy	Preservation and Production of Electronic Records
Policy	Public Information
Policy	Public Records Privacy Protections
Policy	Records Retention
Policy	Student Files/Process Regarding Student Records
Policy	Harassment, Intimidation and Bullying
Policy	Electronic Message Systems
Policy	Employee Conduct
Policy	Harassment
Policy	Bully, Harassment, Intimidation
Policy	Instructional Programs Shared Decision Making
Policy	Student Records
Policy	Student Discipline
Policy	Anti-Virus Guidelines
Policy	Computer Server Security
Policy	Computer Workstation Security
Policy	Network Security
Policy	Web Servers

Legal Reference
18 USC §§ 2510-2522, Electronic Communication Privacy Act

Electronic Resources: Procedure
These procedures are written to support the Electronic Resources Policy of Washington State School for the Blind 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.

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 school 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 school 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 school.

Acceptable network use by school 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 school policies and guidelines;
- Connection of staff personal laptops to the school network after checking with Network Management 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 school students and staff includes but is not limited to:

- Personal gain, commercial solicitation and compensation of any kind;
- Liability or cost incurred by the school;
- Downloading, installation and use of games, audio files video files or other applications (including shareware or freeware) without permission or approval from Network Management;
- 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 school computers, networks and information systems;
- Cyber bullying, including personal attacks or threats toward anyone using online resources originating from locations on or away from the school's campus, **is strictly prohibited and may lead to criminal charges**. If you are aware of cyber bullying, please report it to responsible school personnel;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the school network. Any such equipment will be confiscated and destroyed.

The school 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 school will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the school'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, 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 school web site unless the appropriate permission has been verified according to school 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 school's Internet filter or conceal Internet activity are prohibited: proxies, https, special ports, modifications to school 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 school will be considered SPAM and blocked from entering school e-mail boxes;
- The school 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 school 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 school; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

CIPA/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 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 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.

Ownership of Work
All work completed by employees as part of their employment will be considered property of WSSB. WSSB 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 WSSB. 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 school purposes. Students and staff are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:
- Change passwords according to school policy;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your account password, keep it out of sight;
- 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.

Storage of Sensitive Data and Information
Sensitive information should only be stored within secure network applications such as Skyward, IEP online, and the State of Washington System or on an individual's network drive which is located on a school server. Sensitive information should not be stored on portable storage devices, individual desktop computers, personal web pages/sites, or home computers. Sensitive data/information is any data where the unauthorized access, loss, misuse, modification, or improper disclosure could negatively impact the ability of the school to provide benefits and services to its students or could compromise the privacy of an individual's records. This includes,

but is not limited to, personally identifiable information outside the scope of the school's directory information policies; social security numbers; personal financial information; sensitive plans and procedures; personnel records; individual student records; and student grades Any loss of sensitive information should be reported immediately to the Superintendent.

Portable Storage Devices

Sharing files, copying and moving files, and flexibility with respect to digital information is essential to the instructional process, as well as for disaster recovery and continuity of operations. The School is willing to assume the risk associated with the use of portable storage devices (such as usb drives, laptops, CD-R, DVD-R, pads or slates, iPods, MP3 players, Smart Phones, personal digital assistants such as BrailleNotes and other PDAs, floppy disks, etc.)), and will rely on our antivirus software and other network safeguards to protect our network and digital information.

To provide further protection of the School's network and sensitive information without interfering with the instructional process and academic freedom, the use of portable storage devices— (such as usb drives, laptops, CD-R, DVD-R, pads or slates, iPods, MP3 players, Smart Phones, personal digital assistants such as BrailleNotes and other PDAs, floppy disks, etc.)—must be limited to data that can be made public (in case they are lost or stolen). Private, sensitive data should never be stored on these devices—especially identifiable personal data like social security numbers, health information, student grades, intellectual property, employee and student identities, etc. This applies to any of these devices—even personally owned ones. In the limited cases where potentially sensitive data that should not be made public must be stored on a portable device (such as for disaster recovery or continuity of operations), ITSS approved encryption software must always be used

In the rare event where sensitive data must be stored outside a network application or network drive, the following information is required to process approval of an exception: business or technical justification, scope of data, duration (not to exceed one year), description of potential risks, steps to protect the data.

Student Data is Confidential

School staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

No Expectation of Privacy

The school provides the network system, e-mail and Internet access as a tool for education and research in support of the school's mission. The school 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 school's network. The school reserves the right to disclose any electronic message 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 school 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 school servers nightly – Monday through Friday. Refer to the school retention policy for specific records retention requirements.

Disciplinary Action
All users of the school's electronic resources are required to comply with the school's policy and procedures and agree to abide by the provisions set forth in the school's user agreement.

Violation of any of the conditions of use explained in the school'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.

*Definition of Level 3: High Sensitivity
This category contains the most sensitive data stored at this agency.
This category includes:

- Payment information that is used to authorize or make cash payments to individuals or organizations. This data may be stored in production application files and systems, and includes benefits information, such as payroll information. Such information also includes databases that the user has the authority and capability to use and/or alter to cause an improper payment.
- Proprietary information that has value in and of itself and which must be protected from unauthorized disclosure.
- Computerized correspondence and documents that are considered highly sensitive and/or critical to the agency and which must be protected from unauthorized alteration and/or premature disclosure.
- Records subject to Public Disclosure for which unauthorized disclosure would constitute a "clearly unwarranted invasion of personal privacy" likely to lead to specific detrimental consequences for the individual in terms of financial, employment, medical, psychological, or social standing.
- Information for which either state or Federal laws or regulations require protection or dictate particular handling requirements, for example Health Information Portability and Accountability Act (HIPAA), Executive Order, etc.
- Information that is covered by a contract or agreement in which specific and strict handling requirements are set forth.
- Information for which serious consequences can arise from unauthorized disclosure ranging from life threatening action to legal sanctions.

Washington State School for the Blind

Acceptable Use Form

I understand that use of the Washington State School for the Blind Network is a privilege and I will abide by the "Washington State School for the Blind Acceptable Use of Electronic Resources". I understand that some material contained on the Internet is inappropriate for school use and, therefore, will take personal responsibility not to access this material. I recognize that it is impossible for Washington State School for the Blind to prevent access to all controversial materials, and I will not hold them responsible for materials found or acquired on the network. I further understand that any violation of the regulations in this policy is unethical and may also constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, and appropriate school discipline and/or legal action may be taken.

Name:

Signature: Date:

Alternate Signature Option: Type your name in the text box below if you are unable to apply digital signatures

If Under 13, Parent Signature:

Alternate Parent Signature Option:

Return Signed copy to the following locations:

Employee – HR Department: Anne.Baker@wssb.wa.gov
Student—Irwin Office: Heather.Ratcliff@wssb.wa.gov
Contractor – Business Office: Mary.Sarate@wssb.wa.gov

Washington State School for the Blind
Department of Technology Services