



THE SCHOOL DISTRICT OF WASHINGTON TECHNOLOGY ACCEPTABLE USE POLICY

For the purposes of this procedure and related forms, the following terms are defined:

User – any person who is permitted by the district to utilize any portion of the district’s technology resources, including but not limited to students, employees, School Board members, and agents of the school district.

User ID – any identifier which would allow a user access to the district’s technology resources, to the Internet, or to any program, including but not limited to e-mail access.

Password – a unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

Personal Electronic Devices - Include, but are not limited to, electronic communication equipment such as laptops, portable media players, mobile phones, smart phones, tablet computers and video game devices owned by a student or a student’s parent/guardian.

The following guidelines will be followed by all users of the district’s technology resources. Exceptions will be made for district employees or agents conducting an investigation of student or employee use that potentially violates the law, district policy, rules or procedures. Exceptions will also be made for computer system administrators who need access to district technology resources, and data stored on the district’s resources, maintain the district’s resources or examine and delete data stored on district computers as allowed by the district’s retention policy.

I. General

- a. The use of any Washington School District networked computer is a privilege that may be revoked by instructors, staff, or administrators at any time for abusive or inappropriate conduct. Such conduct would include, but is not limited to, the placing of unlawful information on or through the computer/system; accessing another person’s files or email; installing unauthorized programs or files on a computer or server; and the use of obscene, abusive, or otherwise objectionable language or images in either public or private files or messages.
- b. The district’s Internet access is provided primarily for educational purposes under the direction of district staff. District guidelines prohibit games for entertainment (workstation, network, or Internet based).
- c. The District does not warrant or represent that the district network will meet any specific requirements students may have, or that it will be error-free or uninterrupted. The District will not be liable for any direct or indirect, incidental, or consequential damages (including lost data, information, or profits) sustained or incurred in connection with the use of, operation of, or inability to the District network.
- d. Applying for a user ID under false pretenses is prohibited.
- e. Using another person’s user ID and/or password is prohibited.
- f. Sharing one’s user ID and/or password with any other person is prohibited. In the event a user should share the user ID with another person, whether negligently or intentionally, the user will also be responsible for the actions on the network of that other person.
- g. Deletion, examination, copying or modification of files and/or data belonging to other users without their prior consent is prohibited.
- h. Filtering/Blocking devices are not foolproof, and the district cannot guarantee that users will never be able to access offensive materials using district equipment. Evasion or disabling, or attempting to evade or disable, content-filtering technologies installed by the district is prohibited.
- i. Continued impedance of other users through mass consumption of technology resources, after receipt of a request to cease such activity, is prohibited.
- j. Use of district technology for advertising, commercial purposes or for financial gain is prohibited.
- k. Use of district technology to solicit or announce fund-raising activities for non-profit organizations is prohibited unless authorized by the district.
- l. Accessing fee services without permission from an administrator is prohibited. A user who accesses such services without permission is solely responsible for all charges incurred.
- m. Users are required to obey all laws, including copyright, privacy, defamation and obscenity laws, as a condition of continued access. Users will be held personally liable for any of their own actions that violate these laws.
- n. Accessing, viewing or disseminating information via district resources, including e-mail or Internet access, that is pornographic, obscene, obscene to minors, libelous, pervasively indecent or vulgar, or advertising any product or service not permitted to minors is strictly prohibited.

- o. Accessing, viewing or disseminating information via district resources, including e-mail or Internet access, that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g. threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful school regulations is strictly prohibited.
- p. Any use which has the purpose or effect of discriminating or harassing any person or persons on the basis of race, color, religion, sex, national origin, ancestry, disability, age pregnancy, or use of leave protected by the Family and Medical Leave Act or the violation of any person's rights under applicable laws is strictly prohibited.
- q. Any unauthorized, deliberate, or negligent action which damages or disrupts technology resources, alters its normal performance, or causes it to malfunction is prohibited, regardless of the location or the time duration of the disruption.
- r. All users shall immediately report any security problems or misuse of the district's technology resources to an administrator.
- s. Users may only install and use properly licensed software, audio or video media purchased by the district or approved for use by the district. All users will adhere to the limitations of the district's technology licenses. Copying for home use is strictly prohibited unless permitted by the district's license, and approved by the district.
- t. At no time will computer equipment or software be removed from the district premises, unless authorized by the superintendent or designated school officials.
- u. All users will use the district's property as it was intended. Technology or technology hardware will not be lifted, moved or relocated without permission from the Technology Department. All users will be held accountable for any damage they cause to the district technology resources.
- v. Users shall not plagiarize works that are found on the Internet or any other electronic resource. Plagiarism is defined as presenting the ideas or writings of others as one's own.
- w. The district's technology resources are not a public forum for expression of any kind and are considered a closed forum to the extent allowed by law.
- x. Any user who feels they have a legitimate reason for using the district's technology in a way which may violate any of the district's published policies and procedures (legitimate research, etc.) may request a waiver of the policies and procedures from the building principal, superintendent or their designees. Such waivers shall be granted in accordance with policy EHB.
- y. Rules and regulations of system usage will be added and posted from time to time by the faculty/administrators of the district and/or the network. Users of computers/network are subject to these rules and regulations.

II. Technology Security

- a. Use of district technology resources in attempting to gain or gaining unauthorized access to any computer system or the files of another is prohibited.
- b. Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.
- c. The unauthorized copying of system files is prohibited.
- d. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology are prohibited.
- e. Any attempts to secure a higher level of privilege on the technology resources without authorization are prohibited.
- f. The introduction of computer "viruses," "hacking" tools, or other disruptive/destructive programs into a school computer, the school network, or any external networks is prohibited.

III. On-Line Safety

- a. All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet.
- b. All district employees will abide by state and federal law, and Board policies, including but not limited to policies JO and JO-R, when communicating information about personally identifiable students.
- c. No curricular or non-curricular publication distributed using district technology will include the last name, address, phone number or e-mail address of any student.
- d. Student users shall not agree to meet or meet with someone they have met online without parental approval.
- e. Student users shall promptly disclose to their teacher or another school employee any message the user receives that is inappropriate or makes the user feel uncomfortable.



- f. Users shall receive or transmit communications using only district-approved and district-managed communication systems. For example, users may not use free, web-based e-mail, messaging, videoconferencing or chat services, except in special cases where arrangements have been made in advance and approved by the district.

IV. Electronic Mail

- a. There should be no expectation by any user of the School District of Washington that electronic mail is private. All electronic correspondence is subject to review by administrators or designated district personnel, including messages that are sent or received and review of attachments, and may be subject to “discovery” under litigation.
- b. Forgery (or attempted forgery) of e-mail messages is illegal and strictly prohibited.
- c. Unauthorized attempts to read, delete, copy or modify e-mail of other users are prohibited.
- d. Users are strictly forbidden from sending unsolicited electronic mail to more than one address per message, per day, unless the communication is a necessary, employment-related function, or an authorized publication.
- e. Users must adhere to the same standards for communicating on-line that are expected in the classroom, and consistent with district policies, rules and procedures.

V. Personal Electronic Devices

- a. Possession and use of any personal electronic device is a privilege, not a right, and that violation of these provisions may result in disciplinary action taken against my child including, but not limited to, suspension of my child's access to the district's networks and suspension or expulsion from school.
- b. All use of personal electronic devices during the school day shall be for appropriate educational purposes only and shall be consistent with the educational objectives of the district.
- c. The district may examine devices to the extent allowed by law.
- d. The district assumes no liability for lost, stolen, damaged, or misplaced devices, including those that have been confiscated by district personnel.
- e. Any data plans associated with personal electronic devices must be disabled during the school day, and the device may only connect through the district provided network.
- f. The district is not responsible for any loss of information that may arise from the use of the district's networks, or any resulting loss, injury or damages.
- g. The district will not be responsible for technological support of personal electronic devices, and all devices must be free of viruses before connecting to the district's network.

Crimes

The users of the network are responsible for respecting and adhering to all applicable laws. Any attempt to break those laws through the use of the network and computers may result in criminal prosecution and/or civil litigation, in addition to disciplinary action by the school district. The school district will render all reasonable assistance to law enforcement for the investigation and prosecution of persons who have used this district's technology resources for a criminal purpose or in a criminal manner.

Online Safety

The Federal Trade Commission has some useful privacy pointers for children. More information can be obtained at <http://222.ftc.gov/bcp/conline/edcams/kidzprivacy>.

* * * * *

Note: The reader is encouraged to review related policy EHB-critical for related information in support of this policy area.

TECHNOLOGY USAGE

Employee Technology Agreement

File: EHB-AF3

I have read the school district's Technology Usage Policy (AUP), administrative regulations, and netiquette guidelines and agree to abide by their provisions. I understand that violation of these provisions may result in disciplinary action taken against me, including but not limited to suspension or revocation of my access to district technology, and termination.

I understand that my technology usage is not private and that the school district may monitor my use of district technology, including but not limited to accessing browser logs, e-mail logs, and any other history of use. I consent to district interception of all communications I make or receive using the district's technology resources, pursuant to the Electronic Communications Privacy Act, even if the district's technology resources are accessed remotely.

I understand that the district makes no warranties of any kind, whether express or implied, for the services, products or access it provides. The district's technology resources are available on an "AS IS, AS AVAILABLE" basis. The district is not responsible for loss of data, delays, non-deliveries, mis-deliveries or service interruptions. The district does not guarantee the accuracy or quality of information obtained from the Internet, or use of its technology resources. Access does not include endorsement of content or the accuracy of the information obtained.

I understand I am responsible for any unauthorized costs arising from my use of the district's technology resources. I understand that I am responsible for any damages I incur due to my intentional or negligent use of the district's technology resources.

EMPLOYEE INFORMATION – PLEASE PRINT!		
First Name <small>(As you'd like for it to appear in our system)</small>	Middle Name	Last Name
Position/Subject/Grade Level		Home Building
Employee Signature		Date

* * * * *

Note: The reader is encouraged to review related policy EHB-critical for related information in support of this policy area.