# IN REVISION



**Human Resources**

## Technology

The use of district technology by Everett Public Schools employees is vital to its daily activities. Effective instruction and efficient operation and management require a staff that is skilled in the use of technological tools. Ongoing training is essential.

Additionally, Everett Public Schools permits the use of personal electronic devices ("PEDs", e.g., smartphones, tablets, slates, notebooks, laptops, cellular phones, and other similar mobile electronic devices.) We believe that a PED can play a positive role in furthering our staff and students' learning. The Everett Public Schools wireless network permits individuals with a district network account and a PED to access the Internet.

## Access

Employees will have access to job-appropriate technologies while being provided opportunities to use those technologies.

## Appropriate Use

1. It is the expectation of the district that employees effectively and appropriately use available technology.
2. Inappropriate use should be reported to appropriate district officials.
3. All users of district technology shall comply with current copyright laws (Board Policy 2312 and Procedure 2312P).
4. No user will attempt to breach or modify device hardware and software security measures. Employees will immediately notify the site technician if tampering with the device is suspected.
5. No user will attempt to modify the physical appearance or operating system of any technology equipment. This includes, but is not limited to, unauthorized software updates, and copying or installing non-district licensed software.
6. **Users shall employ Artificial Intelligence (AI) tools and technologies responsibly, adhering to ethical standards, respecting privacy, and complying with district policies and applicable laws.**
7. **Users must critically assess AI-generated content for accuracy and potential biases before utilization and use it ethically with proper documentation and attribution to maintain academic integrity.**
8. **All use of AI tools and technologies must align with district policies and adhere to state and federal laws, with users encouraged to report any misuse or unethical use.**

**Ownership of Work**

All work completed by employees as part of their employment**, including any work involving AI-generated content or tools,** 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. **Employees are responsible for ensuring that AI-generated content is used and attributed in accordance with district policies and ethical standards.**

**General Use of Everett Public Schools Technology**

1. Diligent effort by all users must be made to conserve system resources; e.g., system storage, network bandwidth, software licenses, etc.
2. Prior to having access to district technology, every effort shall be made to provide appropriate training.

**Personal Security**

Staff should not share personal information about employees or students without appropriate authorization. **Additionally, when utilizing AI tools and technologies, staff must ensure that any data inputted or shared complies with data privacy regulations and guidelines, including the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Rule (COPPA), and the Children's Internet Protection Act (CIPA), to safeguard the confidentiality of sensitive information.**

**System Use**

1. All use of district technology**, including AI tools and technologies,** must be in support of education and Everett Public Schools' operations and consistent with the mission of the district. Everett Public Schools reserves the right to prioritize use and access to district technology.
2. Any use of district technology**, including AI tools and technology,** must be in conformity with state and federal law, system use policies and district policy.
3. Use of district technology**, including AI tools,** for commercial solicitation is prohibited except as allowed by law.
4. District technology**, including AI tools,** constitutes public facilities, and may not be used to support or oppose political candidates or ballot measures**, ensuring that AI-generated content remains politically neutral**.
5. Subscriptions to mailing lists, bulletin boards, chat groups, commercial online services or other information services must be directly related to classroom curriculum or the job responsibilities**, including the responsible use of AI tools for educational purposes** ~~**of the employee**~~.
6. **Users must not use district or personal** ~~**District**~~ technology**, including AI tools,** ~~**and/or personal PEDs shall not be used**~~ to disrupt the operation and use of district technology by others. ~~**District technology, including hardware and software, shall not be destroyed, modified, removed or abused in any way.**~~ **Unauthorized modification, removal, or abuse of AI tools or technology components is strictly prohibited.**

7. Use of district technology to develop programs or institute practices that harass other users or gain unauthorized access to any technology service or information and/or damage to the components of a technology service or information are prohibited.
8. Users are responsible for the appropriateness of the material they transmit or publish**, including AI-generated content**. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are prohibited. This may also include the manufacture, distribution, or possession of inappropriate digital images.
9. Use of district technology**, including AI tools,** to access, store or distribute obscene or pornographic material is prohibited.
10. The use of district technology, including cell phones, to conduct and communicate district business via email, district social media and text are all subject to the Washington Public Records Act. Thus, text messaging is limited to district-approved messaging applications, and message content should be limited to classroom reminders, setting up conferencing or notification with parents/guardians, emergencies, safety-related matters or to communicate routine, non-substantive time-sensitive matters.

    Sending phone, email, text, instant messenger, or other forms of written or electronic communication to students when the communication is unrelated to schoolwork or other legitimate school business is prohibited.

    Communications that are one-way and sent to the entire class may be sent directly to students through a district-approved application. If any communication is directed to a small group of students or an individual student, staff shall include a parent/guardian unless doing so would jeopardize the safety, health, or welfare of the student. Staff members should use student school email addresses and the contact information on file for the student including student and parent/guardian contact information from the district student information system and not personally collected contact information, except in an emergency situation.

    If staff members are using online live streaming audio/video platforms e.g., Zoom, Skype, staff will provide prior notice to parents/guardians of when such virtual meetings will take place.
11. Physically connecting or attaching any computer, networking equipment or device to district technology via network ports and/or communications closets, by anyone other than a network technician or other individuals expressly authorized by the director of the Information Systems and Technology Department, is prohibited. Unauthorized computer or networking equipment or components will be removed without notice and immediately investigated for security violations.

**Use of Personal Electronic Devices (PEDs) and Accounts**

Staff may possess and use personal wireless/Wi-Fi PEDs, provided that such devices do not pose a threat to academic integrity, disrupt the learning or work environment, or violate the privacy rights of others. Any district business that is conducted on an employee's personal PED or using personal email or personal social media accounts creates a public record regardless of who owns the PED and whether the account is personal. The district prohibits the conduct of district business using text messaging or personal email or personal social media accounts except in emergencies, safety–related matters, or to communicate routine, non-substantive time-sensitive matters.

Staff in possession of personal PEDs shall observe the following conditions:

1. The Everett Public Schools wireless network will provide filtered Internet access. Everett Public Schools is not liable for access to any other network accessed while the PED is operated in district buildings (including Internet service provided by any commercial service provider). Everett Public Schools will not be responsible for unauthorized financial or resource obligations (i.e., subscriptions and license fees) resulting from the use of, or access to, the district's computer network or the Internet.
2. PEDs shall not be used to violate the confidentiality or privacy rights of another individual, including but not limited to, taking photographs or audio or video recordings of others without their permission or sharing, posting, or publishing photographs, videos, or recordings of others without their permission.
3. Staff are responsible for the personal PEDs they bring to school. The district shall not be responsible for loss, theft, damage, or destruction of PEDs brought onto district property or to district-sponsored or related events or activities. It should be recognized and understood that a PED may not be compatible with district systems. District support staff will provide technical support on a best effort basis only. Access to district systems with a PED is not guaranteed.
4. Everett Public Schools will not be held liable for commercial service charges that occur from the use of an individuals' PED. It is the employee's responsibility to make sure they understand the usage options that are available to them and whether their provider's service plan includes Internet access and all related costs.

**Security**

1. Users are responsible for maintaining the confidentiality of their user IDs and passwords and will not leave an open file or session which is unattended or unsupervised. Account/ID owners are ultimately responsible for all activity and security breaches under their accounts/IDs or via their PED.
2. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, misrepresent other users on district technology or attempt to gain unauthorized access to any data or entity on specific computers or the network.
3. Communications may not be encrypted so as to avoid district security review.
4. Users will avoid using easily guessed passwords and will be required to change passwords regularly (90 days) or as necessary to maintain security.
5. District employees shall not share their passwords with students.

**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. 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 email 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.

**Internet Safety**

Personal Information and Inappropriate Content

A. Staff should not reveal personal information, including a home address and phone number on web sites, blogs, podcasts, videos, social networking sites, wikis, email, or as content on any other electronic medium;

B. 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;

D. If dangerous or inappropriate information or messages are encountered, staff should notify the appropriate school authority; and

E. Be aware that the persistence of digital information, including images and social media activity, may remain on the Internet indefinitely.

**Career and Technical Education (CTE)**

A. Software, equipment, and technology must meet CTE and LITS district standards;

B. CTE equipment and technology must remain in the classroom in which it is deployed. Only CTE field technicians, authorized by LITS or CTE, can remove or relocate CTE equipment and technology;

C. Equipment and technology must be repaired ONLY by authorized CTE field technicians, authorized by LITS or CTE. Unauthorized repairs to CTE equipment and technology can void warranties and/or cause damage;

D. Course frameworks indicate which CTE software is approved and a part of curriculum. New software proposals must be submitted to CTE according to CTE Teacher Handbook; and

E. Software, equipment, and technology require training on proper use and safety prior to purchase, installation and/or deployment.

**Filtering and Monitoring**

Filtering and monitoring technology services are in use on all district technology with access to the Internet using district technology. Filtering and monitoring systems are designed to block or filter access to Internet content the district deems inappropriate, including pornography and any depictions that are obscene or are harmful to minors 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.

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 (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);

C. Email inconsistent with the educational and research mission of the district may be considered SPAM and blocked from entering district email boxes;

D. The district will provide appropriate adult supervision of Internet use while at school. 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;

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; and

F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively.

**No Expectation of Privacy**

It is the policy of Everett Public Schools that district technology is to be used for district-related purposes. Employees have no expectation of privacy when utilizing district technology or when conducting district business using PEDs or accounts.

When responding to a public records request under the Washington Public Records Act, the district will access all district technology to provide a complete response. In addition, the district will access PEDs if the employee has used a personal device, personal email account or personal social media account to conduct district business.

The district reserves the right to inspect, without notice, to review, monitor, and log, as appropriate, all activity using district technology when:

1. It is considered necessary to maintain or protect the integrity, security or functionality of district or other computer resources to protect the district from liability;

2. There is reason to believe that the users have violated this policy or otherwise misused computing resources;

3. An account appears to be engaged in unusual or unusually excessive activity; and
4. It is otherwise required or permitted by law. Additionally, the username and computing services of the individuals involved may be suspended during any investigation or misuse of computer resources.

**District Responsibilities**

Everett Public Schools shall:

1. Review, monitor, and log, as appropriate, all activity on district technology for responsible use consistent with the terms of the policy and procedures.
2. Make determinations on whether specific uses of district technology are consistent with these acceptable use guidelines.
3. Remove a user's access to district technology, with or without notice, at any time the district suspects that the user is engaged in unauthorized activity or violating this policy. In addition, further disciplinary or corrective action(s) may be imposed for violations of the policy.
4. Cooperate fully with law enforcement investigation(s) concerning, or relating to, any suspected or alleged inappropriate activities on district technology or any other electronic media.
5. From time to time, the district will make a determination on whether specific uses of district technology are consistent with the regulations stated above. Under prescribed circumstances, non-student or non-staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district and is authorized by a district administrator.

**Discipline and Consequences for Unauthorized Use of Technology**

Violation of Everett Public Schools' expectations for use of technology may be cause for disciplinary action up to, and including, termination of employment.

| | | |
|---|---|---|
| Cross references: | Board Policy 3245 | Technology |
| | Procedure 3245P | Technology |
| | Board Policy 4400 | Election Activities |
| | Board Policy 5225 | Technology |
| | Board Policy 6550 | Data Security and Privacy |

| | | | |
|---|---|---|---|
| Adopted: | April 2005 | Updated: | February 2020 |
| Revised: | June 2011 | Revised: | April 2020 |
| Updated: | February 2012 | Revised: | June 2020 |
| Revised: | August 2015 | Revised: | February 2023 |
| Updated: | February 2018 | Revised: | April 2023 |
| Revised: | September 2018 | **PROPOSED: March 2024** | |

## Acceptable Use of District Technology

In order to receive access to district technology, this Acceptable Use Policy (AUP) form must first be completed, signed and the original forwarded to the Human Resources Department.

**Everett Public Schools Technology Access**

| Date (print) | First Name | Last Name | Site/Department |
|---|---|---|---|

My signature below indicates that I have read and understand the Everett Public Schools (EPS) Technology Policy 5225 and Procedure 5225P, and that I agree to the conditions of this policy.

Employee signature (required)

My initials below and signature above indicates the following:

| **Statement** | **Initials** |
|---|---|
| I have reviewed a copy of the EPS AUP. | |
| I have read and understand all aspects of the AUP. | |
| I understand that all information stored on the district's computers, networks, and all other district technology is the sole property of EPS. | |
| I understand that I have no expectations of privacy for my use of the EPS's computers, networks, and all other district technology. | |
| I understand that any district business that is conducted on my PED or using personal email or personal social media accounts creates a public record regardless of who owns the PED and whether the account is personal. | |
| I understand that the district limits the conduct of district business using text messaging, personal email, or personal social media accounts. District-approved messaging applications and message content should be limited to classroom reminders, setting up conferencing or notification with parents/guardians, emergencies, safety-related matters, or to communicate routine, non-substantive time-sensitive matters. | |
| **I commit to responsible AI usage, ensuring compliance with data privacy regulations (FERPA, COPPA, CIPA).** | |
| **I support using AI for instructional enhancement, always critically assessing AI-generated content.** | |
| **I pledge to verify AI credibility, prevent misleading content creation, and inform parents about data collection.** | |
| **I will abide by the district's approved list of AI software and tools, recognizing that unauthorized tools may not meet data privacy standards.** | |
| **I will not input personal, sensitive, or confidential data into AI systems without prior parental or guardian authorization, including student education records, while adhering to FERPA, COPPA, and CIPA regulations.** | |
| **I encourage students to use AI tools responsibly for studying and preparation. During assessments or quizzes, I will decide whether AI tool usage is permitted and communicate this clearly.** | |
| **Career Technical Education (CTE) only:** | **Initials** |
| I understand that any equipment and technology purchased by CTE are the property of CTE and may be moved, redeployed, or repaired ONLY by CTE field technicians. | |
| I understand that prior to using or obtaining any new CTE software, equipment, and technology, CTE facilitators must verify that it aligns with my CTE framework. | |
| I understand that I will be properly trained in proper use and safety prior to obtaining and utilizing CTE software, equipment, and technology. | |

Adopted: August 2015
Revised: April 2020
Revised: April 2023
**PROPOSED: March 2024**