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).

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.

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.

System Use

1. All use of district technology 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 must be in conformity with state and federal law, system use policies and district policy.
3. Use of district technology for commercial solicitation is prohibited except as allowed by law.
4. District technology constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
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 of the employee.
6. District technology 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.
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. 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 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.

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	Revised:	September 2018
Revised:	June 2011	Updated:	February 2020
Updated:	February 2012	Revised:	April 2020
Revised:	August 2015	Revised:	June 2020
Updated:	February 2018		

EVERETT PUBLIC SCHOOLS

MANAGEMENT SUPPORT

Data Security and Privacy

It is expected that all employees, volunteers and agents will safeguard student and district data and adhere to the following expectations to protect student and staff privacy and district information as afforded by law.

Definitions

District Data
District data is information created, collected, maintained, transmitted, or recorded by or for the district to conduct district business. It includes data used for planning, managing, operating, controlling, or auditing district functions, operations, and mission; and student and/or staff information created, collected, and maintained by the district including but is not limited to, information in paper, electronic, audio, and visual formats.

Personal Data
Personal data is information created, collected, maintained, transmitted, or recorded by district owned devices, media, or systems that is personal in nature and not related to district business. Personal data includes, but is not limited to, information in paper, electronic, audio, and visual formats. (Staff see Procedure 5225P for Acceptable Use Policy.)

Roles

Data Users
Data users who access district data must comply with: all applicable laws and regulations; district rules, policies, procedures, and standards; and contracts.

Data Managers
Data managers are individuals assigned specific data management responsibilities. They typically have operational responsibility for the management of district data in their functional area.

Data Stewards
Data stewards are designated administrators whose functional areas of responsibility include the creation or origination of and the accessibility to district data. They have overall responsibility for procedures, defining access, managing, and maintaining district data.

Data Governance Group
Data governance group is made up of key data and system stewards who are responsible for the coordination of data entry, security, reporting and accessibility to district data. The group has the responsibility to define, review and promote practices aligned with federal, state, and district policies and procedures.

Chief Information Officer

Chief information officer is responsible for planning and directing strategic, secure, and sustainable use of technology for the purpose of ensuring future use of district-wide instructional, communications and administrative technology is viable. This position coordinates and provides oversight of the data governance group.

Service Providers

Service providers include vendors, strategic partners, higher education institutions or organizations that enter into agreements or contracts with the district. Vendors, partners and outside organizations are responsible to abide by all policies and procedures (research, gift, etc.) and/or enter into contracts that safeguard district data.

Responsibilities

Data Users Responsibilities

Staff members with access to personally identifying information should consider themselves data users and are responsible to ensure the security of data. These responsibilities include:

1. Understand the important of protecting and securing district data as an asset and follow standards and best practices.
2. Understand the use of data in accordance with applicable legal, regulatory, administrative, and contractual requirements; intellectual property or ethical considerations; and strategic or proprietary worth and/or district rules and policies.

Data Manager Responsibilities

Due to job duties and data access, data managers are designated employees who have greater levels of responsibility to ensure the security of data and inform data users. These responsibilities include:

1. Promote the importance of protecting and securing district data as an asset and establish standards and best practices.
2. Attend trainings and remain current regarding the importance of protecting and securing district data as an asset and establish standards and best practices as applied to the stewardship of a specific system.
3. Document and disseminate committee decisions and other relevant information to other data managers and data users.
4. Respond to requests and questions submitted to the district's records office at publicrecords@everettsd.org.

Data and System Stewards Responsibilities

Due to job duties and data access, data and system stewards are designated employees who have greater levels of responsibility to ensure the security of data and train data managers. These responsibilities include:

1. Comply and implement district policies and procedures for the access, use, disclosure, and protection of district data.

2. Provide operational guidance and training regarding data access, use, and compliance with district rules, policies, standards and procedures, as well as applicable legal, regulatory, administrative, and contractual requirements relating to data integrity, security, and confidentiality.
3. Facilitate appropriate district system and data access and relinquishment.
4. Serve as a member of the “data governance group”.
5. Remediate reports of unauthorized data access, misuse, or integrity issues.
6. Report suspected loss, unauthorized access, or exposure of institutional data to the chief information officer.

Data Governance Group Responsibilities

Under the leadership of the chief information officer, the data governance group has the responsibility to review practices and proposals to ensure the security of electronic district data.

1. Provide guidelines for systems requiring integration or use of district data.
2. Create resources to inform and educate data users, data managers and data and system stewards to access and maintain security.
3. Publish and maintain data access procedures and approval processes for managing institutional data.
4. Define methods for ensuring security of district data, contributing to improving security practices, and establishing standards as applied to system stewardship.
5. Facilitate appropriate district system and data access and relinquishment.

Chief Information Officer

The chief information officer has the responsibility for providing leadership to the data governance group.

1. Appoint members to the data governance group.
2. Facilitate the group to ensure the district’s data is secure in a multitude of district and service providers systems.
3. Oversee appropriate district system and data access and relinquishment.
4. Report verified loss, unauthorized access, exposure of institutional data, or data breach to the superintendent.

Records Management

With the enormous amounts of data and concerns for protecting privacy, it is essential that federal, state and district regulations be adhered to in the use and sharing of data, as well as to its destruction.

Data Destruction

To prevent unauthorized disclosure, district data must be properly disposed of using destruction methods that meet the legal, regulatory, and/or district retention requirements. The Local Government Common Records Retention Schedule (CORE) and Public Schools (K-12) Records Retention Schedule provides the requirements for the secure destruction of district data as outlined in the district Business Information Manual.

Public Records

When requests for data are made by the public, the requestor will follow the procedures outlined in Board Policy 4340 Public Access to District Records.

Contract Management

Student and Staff Systems

1. All proposed contracts involving the release or sharing of student and staff data must be submitted to the chief information officer or designee. The chief information officer or designee will convene the data governance team consisting of representation from Learning Management Services, Information Systems and Technology, Business Services and the department or school submitting the contract for review.
2. The default option should be that entities that want access to Everett Public Schools student and staff data shall use the Everett Public Schools contract template.
3. In the event that the entity insists that Everett Public Schools begin with the entity's standard contract (and the entity has the negotiation leverage to insist), the proposed contract shall be reviewed by the chief information officer to determine compliance with law and protection for student privacy.
4. The data governance group will be knowledgeable about the Family Educational Rights and Privacy Act (FERPA), the Children's Internet Protection Act (CIPA), and Children's Online Privacy Protection Act (COPPA) and their associated regulations, as well as Board Policy and Procedure 3600, Student Records, and Board Policy 3250, Release of Directory Information, and the FERPA forms used by Everett Public Schools.
5. The starting point for all contracts will be that no personally identifiable student and staff information will be shared to anyone other than a school official with a legitimate educational interest in the information.
6. If personally identifiable student and staff information must be shared to effectuate the purpose of the contract, the chief information officer or designee will determine if the data shared shall be defined as narrowly as possible and contain contract provisions consistent with Everett Public Schools' obligations under FERPA, a specific FERPA exception applies, or whether parental consent will be necessary.
7. Outside entities will be designated as school officials only in rare cases and only by the chief information officer or designee.
8. All contracts involving the release or sharing of student and staff data shall be maintained by the Business Department in a single location.

9. The chief information officer or designee, in consultation with the Everett Public Schools procurement supervisor and counsel as needed, shall review all contracts to determine whether they contain adequate protections for notification and indemnification of Everett Public Schools in the event of a data breach or violation of student and staff privacy.

Service Providers for Student Use

It is the expectation of school service providers to protect all student personal information they collect, how they use the data and share the student personal information (RCW 28A.604.020). School service means a website, mobile application, or online service that:

a) Is designed and marketed primarily for use in a K-12 school;

b) Is used at the direction of teachers or other employees of a K-12 school; and

c) Collects, maintains, or uses student personal information. A school service does not include a website, mobile application, or online service that is designed and marketed for use by individuals, or entities generally, even if also marketed to a United States K-12 school. A school service provider is an entity that operates a school service to the extent that it is operating in that capacity.

School service providers may collect, use and share student personal information only for purposes authorized by the relevant educational institution or teacher or with the consent of the student or the student's parent or guardian. School service providers may not sell student personal information with the exception of a purchase, merger, or other type of acquisition of a school service provider. School service providers may not use or share any student personal information:

1) For purposes of targeted advertising to students; or

2) To create a personal profile of a student other than for supporting authorized purposes authorized by the relevant educational institution or teacher, or with the consent of the student or the student's parent or guardian.

School service providers must obtain consent before using student personal information in a manner that is materially inconsistent with the school service provider's privacy policy or school contract for the applicable school service in effect at the time of the collection.

In an effort to maintain privacy of student data, these requirements are not to be construed to apply to general audience websites, general audience mobile applications, or general audience online services even if login credentials created for a school service provider's website, mobile application, or online service may be used to access those general audience websites, mobile applications, or online services. It is also not intended to impede the ability of students to download, export, or otherwise save or maintain their own student data or documents.

Cross reference:	Board Policy 6550	Data Security and Privacy	

Adopted:	August 2016	Updated:	December 2018
Updated:	March 2017	Updated:	December 2019
Revised:	May 2018	Updated:	August 2022