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