

PROTECTION OF STUDENT PERSONAL INFORMATION

This procedure will apply to all District contracts with school service providers as defined below. Prior to entering into such contracts and regardless of their form, District employees will consult with the Information Technology Services department to initiate a software approval process which will include the Washington Student Data Privacy Agreement with the service provider. This agreement meets all requirements of Chapter 28A.604, RCW, the Student User Privacy in Education Rights (SUPER) Act and other relevant guidelines.

Only upon successful execution of the agreement shall use of the service or application begin to be used. If the service provider does not complete the agreement, the software may not be used within the District.

Free/Reduced Lunch Status

Student free/reduced lunch status shall not be included in a general student data release and will require a separate Data Sharing Agreement through the Food & Nutrition Services department. These agreements shall be reviewed and approved annually.

Definitions

School service means a website, mobile application, or online service that meets all three of the following criteria: a) it is designed and marketed primarily for use in a K-12 school; b) it is used at the direction of teachers or other employees of a K-12 school and c) it collects, maintains or uses student personal information. This term does not include websites, mobile applications or online services designed and marketed for use by individuals or entities generally, even if also marketed to a K-12 school.

School service provider means an entity that operates a school service.

Student personal information as used in this policy and procedure is consistent with the term as used in Chapter 28A.604, RCW and means:

- information collected through a school service that personally identifies an individual student; OR
- other information collected and maintained about an individual student that is linked to information that identifies an individual student and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

Such information includes, but is not limited to, a student's name, identification numbers, date of birth, demographic information, residence, school student identification number, attendance records, student discipline records, free and reduced lunch information, special education and related services information, standardized test scores and other student growth data. "Information

that personally identifies a student” should be considered synonymous with “personally identifiable information” as that term is used in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232G and 34 C.F.R. Part 99.

Targeted advertising means sending advertisements to a student where the advertisement is selected based on information obtained to infer from a student’s online behavior, application usage, or personal information. It does not include: a) advertising to a student at an online location based upon that student’s current visit to that location without the collection and retention of a student’s online activities over time; or b) adaptive learning, personalized learning or customized education.

Terms of service agreement (otherwise known as a “Click-Wrap” agreement) means an online agreement that requires a user to click to accept the agreement in order to access the service or application for the first time. Once a user clicks “I agree,” the terms will likely govern what information the provider may collect from or about students, how they may use this information, and with whom they will share the information.

Student User Privacy in Education Rights (SUPER) Act requirements

All school service providers must:

- A. Provide the District (including the relevant administrator and/or teacher) with clear and easy to understand information about the types of student personal information it collects and about how it uses and shares student personal information.
- B. Provide the District with prominent notice before making material changes to their privacy policy for school services.
- C. Facilitate parent/guardian access to and correction of student personal information through direct communication with the school service provider or through the appropriate teacher/administrator of the District.
- D. Collect, use and share student personal information only for purposes authorized by the District’s school or teacher consistent with federal and state law and District policy or as authorized in writing by the student’s parent/guardian.
- E. Maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality and integrity of student personal information. The information security program should make use of appropriate administrative, technological, and physical safeguards.
- F. Delete student personal information within a reasonable period of time if the relevant school or district requests deletion of the data under the control of the school unless: 1) the school service provider has obtained student consent or the consent of the student’s parent/guardian to retain information related to that student; or 2) the student has transferred to another school and the receiving school has requested that the school service provider retain information related to that student.

Consistent with federal and state law, school service providers may use student personal information for purposes related to:

- A. Adaptive learning or personalized/customized education;
- B. Maintaining, developing, supporting, improving, or diagnosing the school service provider's website, mobile application, online service, or application;
- C. Providing recommendations for school, educational or employment purposes within a school service, provided that responses are not determined in whole or in part by any payment or other consideration from a third party; or
- D. Responding to a student's request for information or feedback without the information or response being determined in whole in part by payment or other consideration from a third party.

School service providers are prohibited from:

- A. Collecting, using, and sharing student personal information without District authorization consistent with federal and state law and District policies or parent/guardian consent.
- B. Selling student personal information. This prohibition does not apply to the purchase, merger, or acquisition of a school service provider, or to assets of a school service provider by another entity, provided that the successor entity continues to be subject to the same contractual terms as the original school service provider with respect to previously acquired student personal information under the authority of Chapter 28A.604, RCW.
- C. Using or sharing any student personal information for purposes of targeted advertising to students.
- D. Using student personal information to create a personal profile of a student other than for supporting purposes authorized by the school or the teacher or with consent of the student's parent/guardian.
- E. Using student personal information in a manner that is materially inconsistent with the school service provider's privacy policy or its contract with the District or school in effect at the time of collection of the information without obtaining prior consent from the Superintendent or their designee.

The District may permit an exception to the above prohibitions consistent with federal and state law, with the exception of (C) in the above paragraph, on use and disclosure of student personal information by a school service provider to:

- A. Protect the security or integrity of its website, mobile application or online service;

- B. Ensure legal or regulatory compliance or to take precautions against liability;
- C. Respond to or participate in the judicial process as permitted by federal and state law;
- D. Protect the safety of users or others on the website, mobile application or online service;
- E. Investigate a matter related to public safety; or
- F. A subcontractor of the school service provider: 1) contractually requires compliance with federal and state privacy laws and prohibits the subcontractor from using student personal information for any purpose other than providing the contracted service to or on behalf of the school service provider; 2) prohibits the subcontractor from disclosing any student personal information provided by the school service provider to third parties unless the disclosure is expressly permitted by any of the above bulleted items or is used for adaptive learning and customized education purposes pursuant to RCW 28A.604.050 or if consent is obtained in compliance with RCW 28A.604.060, as well as federal and state privacy laws; and 3) requires the subcontractor to comply with all requirements of Chapter 28A.604, RCW.

Adoption Date: May 1, 2019