Procedure - 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 Superintendent or the Superintendent's designee and/or the school or district business officer to verify that any such contract aligns with Chapter 28A.604, RCW, the Student User Privacy in Education Rights (SUPER) Act, as well as any relevant guidelines listed in this procedure.

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 if 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.

Model terms for district and school service provider contracts
The following guidelines are intended to assist contract managers in their review of draft contracts with school service providers and should be read in conjunction with the statutory requirements of chapter 28A.604 RCW, RCW 28A.605.030, and the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g and 34 C.F.R. Part 99, listed above. These guidelines are not intended as a substitute for lawful compliance with federal and state privacy laws protecting personally identifiable student information, consultation with legal counsel, and/or contract legal review.

1. **Definition of Data:**
   Data should be defined broadly to include all information to which providers may have access and specifically should include all student personal information as defined above, information contained in or derived from student education records, metadata, and user content.

2. **Data De-Identification:**
   The "de-identification of data" means the removal of all direct and indirect personal identifiers, including but not limited to a student's name, date of birth, identification numbers, demographic information, residence, school identification number, and other personal information collected and maintained by the District about an individual student that *is linked to* information that identifies an individual student. De-identification means the removal of such information that, alone or in combination with other information 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. Additionally, the school service provider should agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party unless that party agrees not to attempt re-identification.

   Any agreements with contracted school service providers will contain these de-identification requirements and the definitions above.

3. **Marketing and Advertising:**
   Agreements should state the legal prohibition on using or sharing any student personal information for purposes of *targeted advertising to students* (see above) and to also prohibit use of data for targeted *marketing* to students and *marketing or advertising to parents*.

   Avoid language allowing a school service provider to use data to market or advertise to students or

their parents.

4. **Modification of Terms of Service:**
   Consider adding language to state the legal prohibition on the provider changing how it collects, uses or shares data in the agreement in any way without advance notice to the District to require *consent* from the District.

   Avoid language stating that the school service provider will only notify the School/District of *material* changes.

5. **Data Collection:**
   Agreements should limit data collection to only what is necessary to fulfill the agreement if the agreement with the school service provider relates to data protected under the Family Educational Rights and Privacy Act (FERPA), i.e., "Provider will only collect data necessary to fulfill its duties as outlined in this Agreement."

   Avoid any language regarding student user access through a third-party website (such as a social networking site) resulting in the collection of personal information associated with that site.

6. **Data Use:**
   Agreements should restrict the school service provider's *use of data* to the purposes outlined in the agreement.

   Avoid any provision with words to the effect that actions may occur without notice to users.

7. **Data Mining:**
   Consider prohibiting the school service provider from mining data for any purposes other than those agreed to by the parties, as such actions could lead to violations of FERPA or the Protection of Pupil Rights Amendment (PPRA) as well as the provisions of corresponding state law.

   Avoid any language stating that data mining or scanning of user content will occur for the purpose of advertising or marketing to students or parents.

8. **Data Sharing:**
   Consider adding language to the effect that the School/District understands that the school service provider will rely on one or more subcontractors to perform services under this agreement, and that all subcontractors and successor entities of the provider will be subject to the terms of the agreement.

   Avoid language indicating that the school service provider may share information with one or more subcontractors without notice to user.

9. **Data Transfer/Destruction:**
   Consider language requiring the school service provider to ensure that all data in its possession (or that of its subcontractors, agents or any other party to whom the provider has transferred data) will be destroyed or transferred to the School/District when it is no longer needed for the specified purpose, at the request of the School/District.

   Avoid language to the effect that the school service provider maintains the right to use data or user content.

10. **Rights/License to Data:**
    Consider language to the effect of, "the parties agree that all rights, including intellectual property rights, shall remain the exclusive property of the School/District and the school service provider has a limited, nonexclusive license solely for the purpose of performing its obligations in this Agreement. This Agreement does not give the provider any rights, implied or otherwise, to data, content, or intellectual property except as stated in this Agreement. This includes the right to sell or trade data."

    Avoid language to the effect that District data or user content grants the school service provider

with an irrevocable right to license, transmit, or display data or user content.

11. **FERPA Access:**
    Agreements should allow the District to provide parents with access to education records as required by FERPA and Chapter 28A.605 RCW, e.g. “Any data held by provider will be made available to the School/District upon request by the School/District.”

    Avoid language that places barriers (i.e., excessive time for provider response) on the School’s/District’s access to its data held by the school service provider.

12. **Security:**
    Consider (in addition to requiring the school service provider to take administrative, physical and technical safeguards to secure data as required under state law) including provisions such as “industry best practices,” periodic risk assessments, remediation of any identified security vulnerabilities in a timely manner, a written incident response plan, prompt notification of the School/District in the event of a breach, response protocol for a breach, and sharing of incident response plans upon request.

    Avoid contracts that do not reference security controls or those that include a standard other than “industry best practices.”

Adoption Date: **06.22.17**
Classification:
Revised Dates:
Zillah School District