

STILLWATER AREA PUBLIC SCHOOLS

DATA PRIVACY AGREEMENT

ISD#834

AND

Cybersoft Technologies, Inc.

07/20/2022

This Data Privacy Agreement ("DPA") is entered into by and between the Stillwater Area Public Schools ISD 834 (hereinafter referred to as "LEA") and Cybersoft Technologies, Inc (hereinafter referred to as "Provider") on 07/20/2022. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create, and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to the Minnesota Government Data Practices Act ("MGDPA") Minn. Stat. Chapter 13 ; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, MGDPA and other applicable Minnesota State laws, all as may be amended from time to time. In performing services requiring access to private records/data on students, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise

provided by the LEA.

2. Nature of Services Provided. The Provider has agreed to provide the following digital educational products and services described below and as may be further outlined in Exhibit "A" hereto: PrimerEdge and SchoolCafe Child nutrition software and related services

3. Data to Be Provided. The Parties shall indicate the categories of data to be provided in the Schedule of Data, attached hereto as Exhibit "B".

4. DPA Definitions. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. Data Property of LEA. All LEA data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such LEA data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original LEA Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to LEA Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. Separate Account. If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

3. Third Party Request. The Provider will report immediately to the District any requests from third parties for information related to this Contract. Unless agreed otherwise, the District will respond to such data requests. If Provider is subject to compelled disclosure to a third party (e.g. lawfully issued subpoena or court order), Provider must provide timely notification to the LEA in advance of such compelled disclosure.

4. Subprocessors. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect LEA Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. Privacy Compliance. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRa, MGDPA and all other Minnesota privacy statutes.

2. Annual Notification of Rights. If the LEA has a policy of disclosing education records under FERPA (4 CFR § 99.31 (a) (1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its Annual notification of rights.

3. Reasonable Precautions. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. Unauthorized Access Notification. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. Privacy Compliance. The Provider shall comply with all applicable state and federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRa, MGDPA and all other Minnesota privacy statutes. Provider agrees that any information it creates, collects, receives, stores, uses, or disseminates during the course of its performance, which concerns the personal, financial, or other affairs of the LEA, its Board, officers, employees or students shall be kept private and in conformance with all state and federal laws relating to data privacy, including, without limitation, the MGDPA. Provider must comply with any applicable requirements as if it were a governmental entity. The remedies in Minn. Stat. § 13.08 apply to the Provider.

2. Authorized Use. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any LEA Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the LEA Data, without the express written consent of the LEA.

3. Employee Obligation. Provider shall require all employees and agents who have access to LEA Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. No Disclosure. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified LIA Data and not to transfer de-identified LIA Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LIA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. Disposition of Data. Upon written request and in accordance with the applicable terms in subsection a or b, below, Provider shall dispose or delete all LIA Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Disposition shall include (1) the shredding of any hard copies of any LIA Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain LIA Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LIA when the LIA Data has been disposed. The duty to dispose of LIA Data shall not extend to data that has been de-identified or placed in a separate user account, pursuant to the other terms of the DPA. The LIA may employ a "Request for Return or Deletion of LIA Data" form, a copy of which is attached hereto as Exhibit "D". Upon receipt of a request from the LIA, the Provider will immediately provide the LIA with any specified portion of the LIA Data within ten (10) calendar days of receipt of said request.

a. Partial Disposal During Term of Service Agreement. Throughout the Term of the Service Agreement, LIA may request partial disposal of LIA Data obtained under the Service Agreement that is no longer needed.

b. Complete Disposal Upon Termination of Service Agreement. Upon Termination of the Service Agreement Provider shall dispose or delete all LIA Data obtained under the Service Agreement. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LIA that data will not be transferred to a separate account.

6. Advertising Prohibition. Provider is prohibited from using or selling LIA Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LIA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LIA. This section does not prohibit Provider from using Student Data for adaptive learning or customized student learning purposes.

ARTICLE V: DATA PROVISIONS

1. Data Security. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect LJA Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

a. Passwords and Employee Access. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to LJA Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to LJA Data to employees or contractors that are performing the Services. Employees with access to LJA Data shall have signed confidentiality agreements regarding said Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

b. Destruction of Data. Provider shall destroy or delete all LJA Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, or transfer said data to LJA or LJA's designee, according to the procedure identified in Article IV, section 5, above. Nothing in the Service Agreement authorizes Provider to maintain LJA Data beyond the time period reasonably needed to complete the disposition.

c. Security Protocols. Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LJA.

d. Employee Training. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LJA with contact information of an employee who LJA may contact if there are any security concerns or questions.

e. Security Technology. When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

f. Security Coordinator. If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the LIA Data received pursuant to the Service Agreement.

g. Subprocessors Bound. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect LIA Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. Periodic Risk Assessment. Provider further acknowledges and agrees to conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. Data Breach. In the event that LIA Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LIA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall follow the following process:

a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

- i.** The name and contact information of the reporting LIA subject to this section.
- ii.** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- iii.** If the information is possible to determine at the time the notice is provided the number of individuals whose data was potentially subject to the breach and either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
- iv.** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
- v.** A general description of the breach incident, if that information is possible to

determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

- i. Information about what the agency has done to protect individuals whose information has been breached.
- ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Provider agrees to adhere to all requirements in applicable State and in federal law with respect to a data breach related to the LEA Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

e. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of LEA Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.

f. Unless otherwise directed by the LEA, Provider is required to comply with the disclosure requirements of Minn. Stat. 13.055 which requires written notification to any individual whose private data is reasonably believed to have been subject to a breach. The notice must be made in the most expedient time possible and without unreasonable delay, consistent with (1) the legitimate needs of a law enforcement agency; or (2) any measures necessary to determine the scope of the breach and restore the reasonable security of the data. The notice provided must inform the individual: that a report consistent with the requirements of Article V Section 2 (a)-(c) will be developed; how the individual may obtain access to the report; and that the individual may request delivery of the report by mail or email.

g. In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure LEA Data.

ARTICLE VII: MISCELLANEOUS

1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any LEA Data.

2. Termination. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. LEA shall have the right to terminate the DPA and Service Agreement in the event of a material breach of the terms of this DPA.

3. Effect of Termination Survival. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b). Notwithstanding termination of the Service Agreement and prior to destruction of any data as provided in this agreement, the Provider's obligation to comply with applicable state and federal data privacy laws will continue.

4. Priority of Agreements. This DPA shall govern the treatment of LEA data in order to comply with privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. Notice. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement is:

Name: Julie Cink

Title: Finance Director

Contact Information:

The designated representative for the Provider for this Agreement is:

Name: Bhaskar Patel

Title: Vice President

Contact Information:

Bhaskar.patel@cybersoft.net
281 453 8502

6. Entire Agreement. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

7. Severability. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

8. Governing Law; Venue and Jurisdiction. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE IN WHICH THIS AGREEMENT IS EXECUTED, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. Authority. Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of LEA Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the LEA Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the LEA Data and portion thereof stored, maintained or used in any way. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.

10. Waiver. No delay or omission of the LEA to exercise any right hereunder shall be construed

as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

11. Successors Bound. This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this Stillwater Area Public Schools Data Privacy Agreement as of the last day noted below.

Provider:

BY: Bhaskar Patel Date: 07-27-2022

Printed Name: Bhaskar Patel Title/Position: Vice President

Local Education Agency:

BY: Julie Crick Date: 8-9-22

Printed Name: Julie Crick Title/Position: Finance Director

Local Education Agency:

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

- **FULL DESCRIPTION OF SERVICES**

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Metadata	IP Addresses of users, Use of cookies etc.	*
	Other application technology metadata- Please specify:	
Application Use Statistics	Metadata on user interactions with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data- Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
	Employee work attendance	
Communication	Online Communications that are captured (emails, blog entries, phone calls etc.)	
Parent/ Guardian ID	Parent ID number (created to link parents to students)	
Individual Names	First and/ or Last	*
Schedule	Student scheduled courses	
	Teacher names	
	Employee work schedule	
Special Indicator	English language learner information	*
	Low income status	*

	Medical alerts/ health data	
	Student/ Employee disability	
	Special education services (IEP or 504)	
	Living Situations (homeless/ foster care)	
	Other indicator information- Please specify:	
Contact Information	Address	*
	Email	*
	Phone	*
Identifiers	Individual Local (School district) ID	*
	Individual State ID number	*
	Social security numbers	*
	Provider/ App assigned individual ID numbers	
	Individual username	
	Individual passwords	
Transcript	Student course grades	
	Student course data	
	Student performance scores (GPA)	
	Other transcript data- Please specify:	
Transportation	Student bus assignment	

	Student pick up and/ or drop off location	
	Student bus card ID number	
	Other transportation data- Please specify:	
Conduct	Conduct or behavioral data	
Demographics	Data of Birth	*
	Place of Birth	
	Gender	*
	Ethnicity or race	*
	Language information (native, preferred or primary language spoken)	*
	Other demographic information- Please specify:	
Enrollment	Student school enrollment	*
	Student grade level	*
	Homeroom	*
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information- please specify	
User In-App Performance	Program/ application performance (digital assessment and tracking)	
Student program membership	Academic or extracurricular activities a student may belong to or participate in	
Survey Responses	Responses to surveys to questionnaires	

Student/ Employee Artifacts	Student/ Employee generated content; writing; pictures etc.	*
	Other student/ employee artifact data- please specify:	
Employee Records	Benefit data	
	Payroll data	
	Bank information	
	Employment status	
	Previous work history	
	Employee performance data	
Other	Please list each additional data element used, stored or collected by your application	

No LIA Data Collected at this time _____

*Provider shall immediately notify LIA if this designation is no longer applicable.

EXHIBIT “C” DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information (“PII”) from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology (“NIST”) Special Publication Digital Authentication Guideline.

Operator: The term “Operator” means the operator of an Internet Website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. For the purpose of the Service Agreement, the term “Operator” is replaced by the term “Provider.” This term shall encompass the term “Third Party,” as it is found in applicable state statutes.

Personally Identifiable Information (PII): The terms “Personally Identifiable Information” or “PII” shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider’s software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Pupil Generated Content: The term “pupil-generated content” means materials or content created

by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and federal laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

LEA Data: LEA Data includes Student Data as well as any other data elements gather by the Provider or provided by the LEA or its users including but not limited to financial data, employee data, federal ID numbers, and state ID numbers.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and

marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Personal Information: “Personal Information” means information collected through a school service that personally identifies an individual or other information collected and maintained about an individual that is linked to information that identifies an individual. For purposes of this DPA, Personal Information is referred to as LIA Data.

Subscribing LEA: An LIA that was not party to the original Services Agreement and who accepts the Provider’s General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term “Subprocessor” (sometimes referred to as the “Subcontractor”) means a party other than LIA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time.

Third Party: The term “Third Party” means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term “Third Party” when used to indicate the provider of digital educational software or services is replaced by the term “Provider.”

EXHIBIT “D”

DIRECTIVE FOR DISPOSITION OF DATA

_____ directs _____ to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LIA and Provider. The terms of the Disposition are set forth below:

<p>Extent of Disposition</p> <p>Disposition shall be:</p>	<p><input type="checkbox"/> Partial. The categories of data to be disposed of are as follows:</p> <p><input type="checkbox"/> Complete. Disposition extends to all categories of data</p>
<p>Nature of Disposition</p> <p>Disposition shall be by:</p>	<p><input type="checkbox"/> Destruction or deletion of data</p> <p><input type="checkbox"/> Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from IJA that data was successfully transferred, Provider shall destroy or delete all applicable data</p>
<p>Timing of Disposition</p> <p>Data shall be disposed of by the following date:</p>	<p><input type="checkbox"/> As soon as commercially practicable</p> <p><input type="checkbox"/> By (Insert Date) _____</p>



Authorized Representative of IJA

8-9-22
Date

Verification of Disposition of Data
by Authorized Representative of Provider

Date

EXHIBIT "E" DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]



Linda Moncrief <moncriefl@stillwaterschools.org>

Fwd: Online--Stillwater Area PS #834--requesting copy of SchoolCafe Data Privacy Agreement-[#182463]

1 message

John Perry <perryj@stillwaterschools.org>

Thu, Jul 28, 2022 at 4:37 PM

To: Linda Moncrief <moncriefl@stillwaterschools.org>, Shae Seivert <greens@stillwaterschools.org>

Sent from my iPhone

Begin forwarded message:

From: customercare@primeroedge.com
Date: July 28, 2022 at 2:21:16 PM CDT
To: perryj@stillwaterschools.org
Subject: Re: Online--Stillwater Area PS #834--requesting copy of SchoolCafe Data Privacy Agreement-[#182463]
Reply-To: "customercare@primeroedge.com" <customercare@primeroedge.com>

Hello John,

Please see attached signed Privacy agreement from PrimeroEdge. Please let me know if this is sufficient. thanks, Audene

Let us know if you have any questions regarding this ticket by replying all to this ticket

AUDENE CHUNG, MBA, RD
Director, Customer & Expert Care | PrimeroEdge
support: 1.866.442.6030
www.primeroedge.com | customercare@primeroedge.com
Let's Chat ...

Send an email to CustomerCare@primeroedge.com to enable your PrimeroEdge support Chat feature

On Mon, Jul 25 at 8:21 AM , John Perry <perryj@stillwaterschools.org> wrote:
The agreement looks great. Can you send over a signed copy for counter signature?

John Richard Perry
Director of Learning, Technology, and Design Systems
Stillwater Area Public Schools #834
(651) 351-8414

...to inspire curiosity in all learners through educational programming that is personalized, student driven, and highly engaging.

On Sat, Jul 23, 2022 at 12:15 PM customercare@primeroedge.com <customercare@primeroedge.com> wrote:

Hello John Perry,

Please read the full details of this email. The additional information we are needing is located towards the bottom in the information needed section.

This automated email is to let you know that we are awaiting your response from you on the following ticket:

Ticket Number: 182463
Subject: Online--Stillwater Area PS #834--requesting copy of SchoolCafe Data Privacy Agreement

Kindly review the additional clarification given or reply back with the necessary requested information below so we can continue to work on the issue.

Information Needed:

Richard Benson :

Hello John,

I am attaching a copy of your Privacy Agreement. Please let me know if you have any questions.

Thank you,

Let us know if you have any questions regarding this ticket by replying all to this ticket

RICHARD BENSON

Region Lead | PrimeroEdge

support: 866.442.6030

www.primeroedge.com | customercare@primeroedge.com

YOUR GOALS ARE OUR GOALS.

Attachments : 1. Stillwater Privacy Agreement.docx

Thank you,

Cybersoft PrimeroEdge Support Team

 **PEsigned-Stillwater Area PB Privacy Agreement.pdf**
5161K

