

SOUTHWEST WEST CENTRAL SERVICE COOPERATIVE



Education & Administrative Resources

Standard Student Data Privacy Agreement

SWWC Service Cooperative, ISD 991

On the behalf of the participants in

SWWC Data Privacy Program

AND

StoryJumper, Inc.

Effective: 02/18/25

Expires: 02/18/28

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

Southwest West Central Service Cooperative, Independent School District 991, located at 1420 East College Drive, Marshall, MN 56258 (hereinafter referred to as “**SWWC**”), representing itself and the Local Education Agencies participating in the SWWC Data Privacy Program (hereinafter referred to as the “**Local Education Agency**” or “**LEA**”) and
StoryJumper, Inc. located at 2625 Middlefield Road #256 Palo Alto, CA 94306 (hereinafter referred to as “**Provider**”).

WHEREAS, the Provider is providing educational or digital services to one or more LEA participating in the SWWC Data Privacy Program.

WHEREAS, the Provider, SWWC and participating LEA’s recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. §1232g (34 CFR Part 99), the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider, SWWC and participating LEA’s desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

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

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. *Check if Required***
☐ If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is a conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and the Provider Terms of Service or Privacy Policy, the terms of this DPA shall control.
4. This DPA shall stay in effect for three years.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices**. All notices or other communication required or permitted to be given hereunder

may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this Agreement is:

Josh Sumption, Chief Technology and Information Officer
SWWC Service Cooperative – SWWC Data Privacy Project
1420 E College Drive
Marshall, MN 56258
Phone: 507-537-2240 Email: data.privacy@swwc.org

The designated representative for the Provider for this Agreement is:

Name: John Yen

Title: CEO

Mailing Address:

2625 Middlefield Road #256 Palo Alto, CA 94306

Phone: 650-330-1133


Email: privacy@storyjumper.com

IN WITNESS WHEREOF, SWWC, on behalf of all participating LEA's, and Provider execute this DPA as of the Effective Date.

SWWC:

By:  Date: 3/17/2025
Josh Sumption, Chief Technology and Information Officer

Provider:

By:  Date: 02/18/25

Printed Name: John Yen

Title/Position: CEO

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **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 the terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies, etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student 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 Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student 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. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the user of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law, the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the timeframe required under state law for an LEA to a parent or student, whichever is sooner) to the

LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a sperate account created by the student.
4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining Services in compliance with all applicable federal, state, and local privacy laws, ruled, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 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 Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known 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 federal, state and local laws, rules and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligations.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not sell Student Data to any third party.
5. **De-Identified Data.** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for the adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive the termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any parties unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which re-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no

written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II.3. The LEA may employ a “**Directive for Disposition of Data**” form, a copy of which is attached hereto as **Exhibit “D”**. If the LEA and Provider employ **Exhibit “D”**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit “D”**.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers of LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DEPA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days’ notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider’s facilities, staff, agents and LEA’s Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
3. **Data Security.** The Provider agrees to utilize administrative, physical and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The Provider shall implement an adequate Cybersecurity

Framework based on one of the nationally recognized standards set forth in **Exhibit “F”**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit “H”**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “F”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who SWWC or LEA may contact if there are any data security concerns or questions.

4. **Data Breach.** In the event of an unauthorized release, disclosure, or acquisition of Student Data that compromises the security, confidentiality, or integrity of the Student Data maintained by the Provider shall provide notification to SWWC and the LEA withing seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as becomes available:
 - i. The name and contact information of the reporting LEA 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 the breach.
 - iii. If the information is possible to determine at the time the notice is provided, then 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 was provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
 - (3) 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 Student Data or any portion thereof, including personally identifiable information and agrees to provide SWWC or LEA, upon request, with a summary of said written incident response plan.

- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) 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 Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

By signing this agreement, Provider is offering the Privacy Terms defined herein to all LEA's participating in and represented by the SWWC Data Privacy Program.

ARTICLE VII: MISCELLANEOUS

1. **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. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of the LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H, will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Entire Agreement.** This DPA and the Service Agreement constitute 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.
5. **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.

6. **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.
7. **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.
8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees, or contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be constructed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT “A”

DESCRIPTION OF SERVICES

StoryJumper is a website that offers students and teachers the opportunity to read, write, illustrate, voice narrate, publish, share, and sell their own books.

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.	X
	Other application technology metadata- Please specify:	
Application Use Statistics	Metadata on user interactions with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data- Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online Communications that are captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Data of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, 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:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID Number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information – Please specify:	
Student Contact Information	Address	
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last	X

Student In App Performance	Program/ application performance (typing programming student types 60 wpm, reading program-student reads below grade level)	
Student program membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys to questionnaires	X
Student work	Student generated content; writing, pictures, etc.	X
	Other student work data – Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades / performance scores	
	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:	
Other	Please list each additional data element used, stored or collected by your application:	
None	No Student Data collected at this time. Provider shall immediately notify SWWC if this designation is no longer applicable.	

EXHIBIT “C”

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provider that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such 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.

Meta Data: means information that provides meaning and context to the data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

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 for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with the LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

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 Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Student Generated Content: The term “Student-Generated Content” means materials or content created by a student in the services 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 student content.

School Official: For the purposes of this DPA 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 Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

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, birthdate, home or other physical 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 identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state and local 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.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve the service, and who has access to Student Data.

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet website, online service, or mobile application by such student or the retention of such

student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet website based on the content of the web page or in response to a student's response or request for information or feedback.

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 Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, 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

{Insert Name of District or LEA} directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable

_____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT “F”
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

2/24/2020

The Education Security and Privacy Exchange (“Edspex”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* (“Cybersecurity Frameworks”) that may be utilized by Provider.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
X	International Standards Organization (ISO)	Information technology – Security techniques – Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD (A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here.

EXHIBIT "G"
Supplemental SDPC State Terms for Minnesota
Version 1.0

This **Exhibit G**, Supplemental SDPC State Terms for Minnesota ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between Southwest West Central Service Cooperative ("SWWC") on behalf of itself and all LEA's participating in and represented by the SWWC Data Privacy Program, and _____ StoryJumper, Inc. _____ (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Compliance with Minnesota Privacy Laws.** In performing its obligations under the Agreement, the Provider shall comply with all Minnesota laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the regulations defined in the Minnesota Government Data Practices Act, specifically those regulations defined in Minn. Stat. § 13.32 (2022), and all references therein.
2. **Definition of "Student Data."** In addition to the definition set forth in Exhibit C, Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Minnesota law and regulations, including but not limited to (a) "educational data," as defined in Minn. Stat. §13.32.1, Subdivision 1 (2022).
3. **School Official Designation.** Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.
4. **Limitations on Re-Disclosure.** The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under Minn. Stat. § 13.32 (2022), FERPA, or any other applicable laws or regulations. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the other party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five

(5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.

5. **Notices.** Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.
6. **Corrections to Factual Inaccuracies.** In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.
7. **Security Breach Notification.** In addition to the information enumerated in Article V, Section 4(1) of the DPA Standard Clauses, any Security Breach notification provided by the Provider must adhere to the following procedures:
 - a. In the event where a direct contract between the LEA and Provider exists shall include:
 - i. A list of the LEA's and students whose Educational Data was involved or is reasonably believed to have been involved in the breach, if known; and
 - ii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.
 - b. In the event where a direct contract between the LEA and Provider does not exist and the Provider is providing services strictly under the conditions of this DPA, the Provider must send to SWWC a notification of the Security Breach that includes the following:
 - i. A list of known LEA's where student data was involved or is reasonably believed to have been involved in the breach.
 - ii. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.
8. **DPA Governance.** This DPA shall cover and provide protections delineated within to all current and future LEAs that have entered into agreements with the Southwest West Central Service Cooperative for its Data Privacy Program.
 - a. **Term of Coverage for LEA.** LEA's participating in the SWWC Data Privacy Program are covered by this DPA as long as their membership in the Data Privacy Program remains in good standing. A LEA that chooses not to renew its

membership in the SWWC Data Privacy Program will lose its coverage by this DPA after June 30 of the final contracted year.

9. **Termination.** Paragraph 1 of Article VII shall be deleted, and the following shall be inserted in lieu thereof: “In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.’
10. **Transfer or Deletion of Student Data.** The Provider must destroy or return to the appropriate educational agency all educational data created, received, or maintained pursuant or incidental to the contract within 90 days of the expiration of the contract.
11. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider’s products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.
12. **Provider Conditions for Minimal Age.** The provider must indicate the minimum age of users of the product covered by this DPA. If parental consent is required for use of the product, the provider must also indicate the minimum age of users of the product when parental consent is given. LEA acknowledges that all users of the product will meet the minimum age requirements provided in this agreement.

Minimum age of product users without consent: N/A

Is written parental consent required for users of this product under the minimum age of users for whom consent has not been provided?

 yes X no

Minimum age of product users with written consent: N/A

13. **Provider Conditions for Geolocation Tracking.** The provider must indicate if the product covered by this DPA tracks the geolocation of student users. If the covered product does track the geolocation, the provider must indicate if the geolocation tracking functions can be administratively disabled for student users. The provider may optionally provide additional information regarding geolocation tracking capabilities of the covered product.

Does your product track and store the geolocation of users? yes X no

If "yes" was selected - Does your product offer the ability to
administratively disable geolocation tracking? _____ yes _____ no

Please provide any additional information regarding Geolocation tracking capabilities of your
product: