

ILLINOIS STUDENT DATA PRIVACY  
AGREEMENT Version 1.0 (December 11, 2018)

School District/Local Education Agency: \_\_\_\_\_

AND

Provider: \_\_\_\_\_

Date: \_\_\_\_\_

This Illinois Student Data Privacy Agreement ("DPA") is entered into by and between the \_\_\_\_\_ (hereinafter referred to as "LEA") and \_\_\_\_\_ (hereinafter referred to as "Provider") on the \_\_\_\_\_. The Parties agree to terms as stated herein.

## RECITALS

**WHEREAS**, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital education 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 Education Rights and Privacy Act ("FERPA") at 20 U.S.C. §1232g (34 C.F.R. 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 Illinois State student privacy laws, including the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/; 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; and

**WHEREAS**, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in Illinois the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

**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 Student Data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, ISSRA, MHDDCA, SOPPA, IPA, PIPA, and other applicable Illinois State laws, 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 performing services otherwise undertaken by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of 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:
3. **Student Data to be Provided.** The Parties shall indicate the categories of Student 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. **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 Agreement 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 Student Data contemplated pursuant to the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and ISSRA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures pursuant to which a parent, legal guardian, or eligible student may review and/or copy Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a timely manner (and no later than 10 business days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to review or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review and/or copy any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, which will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** In the event 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 that, such transfer shall only apply to pupil generated content that is severable from the Service.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request (including subpoena) for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to seek the data directly from the LEA. Provider shall notify the LEA at least five school days in advance of a court ordered disclosure to a Third Party and shall provide the LEA with a copy of the court order requiring such disclosure.

5. **Subprocessors.** Provider shall enter into written agreements with any and all Subprocessors performing functions pursuant to the Service Agreement. Such agreements shall require the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA. Provider shall make all written agreements with Subprocessors performing functions pursuant to the Service Agreement available for inspection and copying by the LEA upon request.

### 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, ISSRA, MHDDCA, SOPPA, IPA, PIPA, and all other applicable Illinois privacy statutes.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing education records under FERPA (34 C.F.R. § 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 obtaining 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, ISSRA, MHDDCA, SOPPA, IPA, PIPA, and all other applicable Illinois privacy statutes.
2. **Authorized Use.** The data made available 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 and applicable implementing regulations referred to above in subsection 1. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student 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 Student data, without the express written consent of the LEA.
3. **Employee Obligation.** Provider shall, by written acknowledgment, require all employees and agents who have access to Student 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 C.F.R. § 99.31(b). Provider shall not attempt to re-identify de-identified Student Data and shall not transfer de-identified Student 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 LEA which 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 below in subsections a. or b., Provider shall dispose or delete all Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. The method of disposition shall include: (1) the shredding of any photocopies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or electronic/digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" form, a copy of which is attached hereto as Exhibit "D." Within ten (10) calendar days after the date of a request from the LEA, the Provider shall provide the LEA with any specified portion of the Student Data.

- a. **Partial Disposal During Term of Service Agreement.** Throughout the Term of the Service Agreement, LEA may require partial disposal of Student Data that is no longer needed which was obtained pursuant to the Service Agreement. Partial disposal of data shall be subject to LEA's request to transfer data to a separate account, pursuant to Article II, section 3.

- b. **Complete disposal Upon Termination of Service Agreement.** Upon Termination of the Service Agreement, Provider shall dispose of or delete all Student Data obtained under the Service Agreement. Prior to disposition of the data, Provider shall notify LEA in writing of its option to transfer data to a separate account, pursuant to Article II, section 3. In no event shall Provider dispose of data pursuant to this provision unless and until Provider has received affirmative written confirmation from LEA that the data will not be transferred to a separate account.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to: (a) market or advertise to students or their 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 LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. 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 shall abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by unauthorized persons or entities. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. The applicable measures shall include, but are not limited to the following:

- a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3, and as it may be amended or replaced from time to time. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. 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 Student 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 LEA or LEA's designee, according to the procedure identified in Article IV, section 5. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition.
- c. **Security Protocols.** The parties shall maintain security protocols that meet industry standards regarding 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 LEA.
- d. **Employee Training.** The Provider shall provide periodic security and Student Data training to those of its employees who operate or have access to the system. In addition, Provider shall provide LEA with contact information of an employee who LEA 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 Student Data received pursuant to the Service Agreement.
- g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Upon request, Provider shall make all written agreements with Subprocessors performing functions pursuant to the Service Agreement available for inspection by the LEA. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

- h. Periodic Risk Assessment.** Provider shall conduct periodic (no less than semi-annual) digital and physical risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.
- 2. Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. Provider shall undertake 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 2a. shall include, at a minimum, the following information:
    - 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 a 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 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 federal law 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.
  - 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 Student Data or any

portion thereof, including personally identifiable information, and it agrees to provide LEA, upon request, with a copy of such written incident response plan.

- f. Provider is prohibited from directly contacting a parent, legal guardian or eligible pupil unless expressly requested by LEA. If LEA requests Provider's assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to Provider, Provider shall notify the affected parent, legal guardian, or eligible pupil of the unauthorized access, which shall include the information listed in subsections b. and c. hereof. If requested by LEA, Provider shall reimburse LEA for costs incurred to notify parents/families of a breach not originating from LEA's use of the Service.
- 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 Student Data.

## **ARTICLE VI – GENERAL OFFER OF PRIVACY TERMS**

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this DPA to any other LEA who signs the acceptance on said Exhibit. The Form is limited by the terms and conditions described therein.

## **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 Student 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 II, section 3, and Article V, section 1b.
4. **Priority of Agreements.** This DPA shall govern the treatment of student 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 section 4, all other provisions of the Service Agreement shall remain in effect.
5. **Limited Authority to Renegotiate.** Notwithstanding any other provision of this Agreement, if any federal, state, or local government or agency passes, issues, or promulgates any law, rule, regulation, standard of interpretation, or materially changes its current position as to the interpretation of any existing law, rule, regulation or standard, including but not limited to FERPA, PPRA, COPPA, ISSRA, MHDDCA, SOPPA, IPA, or PIPA, at any time while this Agreement is in effect in a manner that would prohibit, restrict, limit or render illegal the relationship described herein, or if any governmental entity issues a written allegation or otherwise provides notice to the parties to the effect that the relationship described herein is in violation of any law, rule or regulation, then either party may give the other party notice of intent to amend this Agreement to bring it into



compliance with all applicable laws. If this Agreement is not amended in writing by mutual agreement within thirty (30) days after notice is given, then the party giving notice shall have the right to terminate the Agreement effective at the end of the thirty (30) day renegotiation period.

6. **Notice.** All notices or other communication required or permitted to be given hereunder shall 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 representative. Any notice delivered hereunder shall be deemed effective, as applicable, upon delivery, if personally delivered; 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.

**a. Designated Representatives**

The designated representative for the LEA for this Agreement is:

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Contact Information:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

The designated representative for the Provider for this Agreement is:

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Contact Information:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

- b. Notification of Acceptance of General Offer of Terms.** Upon execution of Exhibit E, General Offer of Terms, Subscribing LEA shall provide notice of such acceptance in writing and by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, to the designated representative below. Any notice delivered hereunder shall be deemed effective, as applicable, upon delivery, if personally delivered; 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.

The designated representative for the notice of acceptance of the General Offer of Privacy Terms is:

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Contact Information:

---

---

---

7. **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 at any time.
8. **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 interpreted 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 interpreted without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
9. **Governing Law: Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF ILLINOIS, 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 THE LEA IS LOCATED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
10. **Authority.** Provider represents that it is authorized to be bound to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained herein, all related or associated institutions, individuals, employees, contractors, subcontractors or subprocessors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and/or portion thereof stored, maintained, or used in any manner whatsoever. Provider agrees that any purchaser of the Provider shall also be bound to the Agreement.
11. **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.
12. **Successors Bound.** This DPA is and shall be binding upon the respective assigns or 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 Provider.

**13. Assignment.** Neither Party nor any subsidiary, successor, partner, employee, agent or affiliate shall assign or delegate any of the rights or responsibilities under this Agreement without the prior written consent of the other, which shall not be unreasonably withheld.

*[Signature Page Follows]*

**IN WITNESS WHEREOF**, the parties have executed this Illinois Student Data Privacy Agreement as of the last day noted below.

Provider:

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

Local Education Agency:

BY: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

***Note: Electronic Signature not permitted.***

**EXHIBIT "A"**

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE. IF MORE THAN ONE PRODUCT OR SERVICE IS INCLUDED, LIST EACH PRODUCT HERE.]

## EXHIBIT “B”

### SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users. Use of cookies, etc.	
	Other application technology meta data- Please specify:	
Application Use Statistics	Meta data on user interaction with application	
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)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	

Category of Data	Elements	Check if used by your system
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	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:	

Category of Data	Elements	Check if used by your system
Parent/Guardian Contact Information	Address	
	Email	
	Phone number	
	State ID Number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
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	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/health data	
	Student disability information	

Category of Data	Elements	Check if used by your system
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information – Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID Work data- Please specify:	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-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 or questionnaires	

Category of Data	Elements	Check if used by your system
Student work	Student generated content; writing, pictures, etc.	
	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 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. If additional space is needed, use space below.	



No Student Data Collected at this time\_\_\_\_\_.

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

OTHER: Use space below, if more space is needed:

## **EXHIBIT “C”**

### **DEFINITIONS**

**Commercial Purpose:** Using information for a commercial purpose means to advance a person’s commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction.

**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.

**IPA:** The Identity Protection Act, 5 ILCS 179/.

**ISSRA:** The Illinois School Student Records Act, 105 ILCS 10/.

**MHDDCA:** The Illinois Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/.

**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 hereafter in the definition of Student Data.

**PIPA:** The Personal Information Protection Act, 815 ILCS 530/.

**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 C.F.R. § 99.31(a)(1)(B), a School Official includes 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 education records.

**SOPPA:** The Student Online Personal Protection Act, 105 ILCS 85/.

**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 identifiers, 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 Illinois 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 the information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

**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.

**Student Personal Information:** “Student Personal Information” 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, as identified by Washington Compact Provision 28A.604.010. For purposes of this DPA, Student Personal Information is referred to as Student Data.

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

**Subprocessor:** For purposes of this Agreement, 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 its software, and who has access to PU.

**Targeted Advertising.** Targeted advertising means presenting advertisements to a student where the advertisement is selected based on information obtained or inferred over time from that student's online behavior, usage of applications, or covered information. For purposes of this definition, "covered information" means personally identifiable information or material or information that is linked to personally identifiable information or material in any media or format that is not publicly available.

**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 LEA and Provider. The terms of the Disposition are set forth below:

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

\_\_\_\_\_  
Authorized Representative of LEA

\_\_\_\_\_  
Date

\_\_\_\_\_  
Verification of Disposition of Data  
by Authorized Representative of Provider

\_\_\_\_\_  
Date

## **EXHIBIT "E"**

### **GENERAL OFFER OF PRIVACY TERMS**

#### **1. Offer of Terms**

Provider offers the same privacy protections found in this DPA between it and \_\_\_\_\_, dated \_\_\_\_\_, to any other LEA ("Subscribing LEA") which accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider in Exhibit "B" to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of any of the following: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify \_\_\_\_\_ in the event of any withdrawal so that this information may be transmitted to the appropriate users.

Provider: \_\_\_\_\_

By: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

#### **2. Subscribing LEA**

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Subscribing LEA:

By: \_\_\_\_\_ Date: \_\_\_\_\_

Printed Name: \_\_\_\_\_ Title/Position: \_\_\_\_\_

**TO ACCEPT THE GENERAL OFFER, THE SUBSCRIBING LEA MUST DELIVER THIS SIGNED EXHIBIT TO THE PERSON AND EMAIL ADDRESS LISTED BELOW.**

**Name:** \_\_\_\_\_

**Title:** \_\_\_\_\_

**Email Address:** \_\_\_\_\_

**EXHIBIT “F”**

DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]