

SchoolMint Student Data Privacy Agreement

This Student Data Privacy Agreement (“DPA”) is entered into by and between the local educational agency (hereinafter referred to as “LEA”) and SchoolMint, Inc. (hereinafter referred to as “Provider”) on the date that this DPA is duly executed, as indicated below. The Parties agree to the terms stated herein.

BACKGROUND

1. The Provider has agreed to provide the LEA with certain digital educational services (“Services”) pursuant to a duly executed contract (“Service Agreement”); and
2. 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 and 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
3. The documents and data transferred from LEAs and created by the Provider’s Services are also subject to all applicable state student privacy laws; and
4. For the purposes of this DPA, Provider is a school district official, as defined pursuant to 34 CFR 99.31 (B), with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and
5. 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
6. The Provider may, by signing the “General Offer of Privacy Terms” (“Exhibit B”), agree to allow other LEAs 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.
7. In accordance with the above, for good and valuable consideration, the Parties agree as follows herein.

DEFINITIONS

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.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, including personally identifiable information 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 as specified in "Exhibit A" 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 deidentified, or anonymous usage data regarding a student's use of Provider's services.

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.

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, and applicable state law, all as may be amended from time to time. In performing these services, the Provider shall be considered a School District Official with a legitimate educational interest, and performing services otherwise provided 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 one or more digital Strategic Enrollment Management (SEM) products and services to attract, enroll, and retain K12 student enrollment. Provider employees will have no direct contact with students in the provision and servicing of these products and services.
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 A". The LEA shall provide the categories of data described in "Exhibit A", which LEA shall be solely responsible for adhering thereto.

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 per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School District Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. 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 by which a parent, legal guardian, or eligible student may review or view Student Data in the pupil's records, request an amendment to information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Throughout the term of the Service Agreement and 30 days after, the LEA will be able to gain access, download, and amend all student data. In the event that a parent of a pupil 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. **Third Party Request.** Should a third party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the third party to request the data directly from the LEA. Provider shall notify the LEA as soon as possible in advance of a compelled disclosure to a third party (e.g., a subpoena), unless prohibited by a legal authority, if permissible under the circumstances.

4. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA, as well as state and federal law.

III. DUTIES OF LEA

1. **Privacy Compliance.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, and applicable state law.

2. **Annual Notification of Rights.** The LEA shall include a specification of criteria under FERPA 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.

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, PPRRA, and applicable state law.

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 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 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. Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless that party agrees in writing not to attempt re-identification (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer.

4. **No Disclosure**. 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 or upon termination of the Service Agreement, Provider shall dispose of or delete all Student Data obtained under the Service Agreement and in accordance with the applicable terms below. Provider shall dispose of or delete all Student 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 student 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 Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall dispose of all data 30 days after the termination of the Service Agreement, and shall notify LEA once it has done so. The duty to dispose of Student Data shall not extend to data that has been de-identified pursuant to the other terms of the DPA. Upon receipt of a request from the LEA, the Provider will immediately provide the LEA with confirmation of the deletion of any specified portion of the Student Data within ten (10) calendar days of receipt of said request.

6. **Advertising Prohibition.** Provider is prohibited from using or selling Student Data to (a) market or for targeted advertising 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 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.

V. DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology standard practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. These measures shall include, but are not limited to:

- a. **Passwords and Employee Access.** Provider shall secure Provider issued usernames and passwords, employee usernames and passwords, and any other means of gaining access to the Services or to Student Data. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student 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 Student Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained. Nothing in the Service Agreement authorizes Provider to maintain Student Data beyond the time period reasonably needed to complete the disposition detailed herein.
- 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 LEA.
- 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 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, data back-ups, 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 Section VII.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. **Subcontractors Bound.** Provider shall enter into written agreements whereby Subcontractors agree to secure and protect Student Data in a manner consistent with the terms of this Section V.
 - h. **Periodic Risk Assessments.** Provider further acknowledges to remediate any identified material security and privacy vulnerabilities in a timely manner that are identified through internal risk assessments (digital and physical).
 - i. **Audits.** Upon receipt of a request from the LEA, the Provider will allow the LEA to audit non-confidential documentation pertaining to security and privacy measures that are in place to ensure protection of the Student Record or any portion thereof to the extent available to Provider. The provider will also acknowledge and work with any state or federal organization or agency who has authority over student data or the LEA has contracted with to review said non-confidential documentation pertaining to security and privacy measures.
2. **Data Breach.** In the event that Student Data is accessed, Provider shall provide prompt notification to LEA within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours of confirmation of a data breach. Provider shall provide the following at the time of notification:
- a. The security breach notification 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. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
 - i. Whether the notification was delayed because of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

- ii. Provider agrees to adhere to all requirements in applicable state law and federal law with respect to a data breach related to the Student Data, including, when appropriate or required.
 - a. Provider further acknowledges and agrees to, upon request at reasonable times, to answer questions on non-confidential information regarding security protocols and/or safeguards.
 - a. 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. Provider agrees to answer non-confidential questions about said incident response plan.
 - a. Provider is prohibited from directly contacting parent, legal guardian or eligible pupil unless expressly requested by LEA.
 - a. 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.

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 B"), be bound by the terms of this DPA to any other LEA who signs the acceptance in said Exhibit. The Form is limited by the terms and conditions described therein.

VII. GENERAL TERMS

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 Section V.1(b), and Section II.3 above.
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 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 and delivery is verified by the receiving party), or first-class mail, postage prepaid, sent to the designated representatives before:

a. Designated Representatives

The designated representative for the LEA for this Agreement may be identified in LEA's Order Form, if elected. The designated representative for the Provider for this Agreement is:

Name: **Zach Hollwedel**
Title: **SVP, Business Operations**

Contact Information:
Email - zach.hollwedel@schoolmint.net

b. Notification of Acceptance of General Offer of Privacy Terms. Upon execution of "Exhibit B", General Offer of Privacy Terms, Subscribing LEA shall provide notice of such acceptance 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, to the designated representative below.

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

Name: **Zach Hollwedel**
Title: **SVP, Business Operations**

Contact Information:
Email - zach.hollwedel@schoolmint.net

6. **Entire Agreement.** Subject to the terms and conditions of the underlying SchoolMint Master Services Agreement, this DPA constitutes the entire agreement of the Parties relating to the handling of Student Data 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 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 IN WHICH LEA IS LOCATED AND UTILIZING PROVIDER'S PRODUCTS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS IN THE STATE AND COUNTY IN WHICH LEA IS LOCATED AND UTILIZING PROVIDER'S PRODUCTS, FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA.

9. Authority. Provider represents that it is authorized to bind to the terms of this Agreement, 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, or may own, lease or control equipment or facilities of any kind where the Student 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.

***** Signatures On The Following Page *****

IN WITNESS WHEREOF, the signatories to this DPA are authorized to enter into binding agreements on behalf of each Party respectively. The Parties have executed this Student Data Privacy Agreement as of the last day noted below.

SchoolMint, Inc.:

BY: _____

Date: _____

Printed Name: _____ Title/Position: _____

Local Education Agency:

BY: _____

Date: _____

Printed Name: _____ Title/Position: _____

EXHIBIT A

Category of Data	Elements	Check if Data is Required
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
Enrollment	Student school of enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor name	
	Specific curriculum programs	
	Year of graduation	
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	
Special Indicator	English language learner information	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	

	Living situations (homeless/foster care)	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (e.g., 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	
Student work	Student generated content such as writing, pictures, etc.	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	

EXHIBIT B

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and the above-referenced LEA to any other LEA (“Subscribing LEA”) who 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 its sole discretion.

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: _____