STUDENT DATA PRIVACY ADDENDUM

This Student Data Privacy Addendum ("**Addendum**") supplements our Terms of Service for an Educational Institution customer ("**Customer**") that makes the Lupin Learn Student features and services ("Services") available to Students for use in an educational setting. Capitalized terms that are not defined in this Addendum have the meaning set out in our Terms of Service.

If Lupin Learn ("**Provider**") and Customer have agreed in writing to separate terms reasonably equivalent to this Addendum, then the parties agree that those terms will apply instead of this Addendum.

The purpose of this Addendum is to establish Provider's and Customer's respective obligations and duties in order to protect personally identifiable student information and comply with 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 Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. § 1232h; 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.

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of Addendum**. The purpose of this Addendum 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 the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing Services otherwise provided by the LEA (34 CFR § 99.31(a)(1)). Provider shall be 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 herein, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "A"**.

3. **Definitions**. The definition of terms used in this Addendum is found in **Exhibit "B".** In the event of a conflict, definitions used in this Addendum shall prevail over terms used in any other writing, including, but not limited to any Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of Customer**. All Student Data transmitted to Provider pursuant to this Addendum is and will continue to be the property of and under the control of Customer. Provider further acknowledges and agrees that all copies of such Student Data transmitted to Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Addendum 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 Addendum, shall remain the exclusive property of Customer. For the purposes of FERPA, Provider shall be considered a School Official, under the control and direction of Customer as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access**. To the extent required by law Customer 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 time frame required under state law for Customer to respond to a parent or student, whichever is sooner) to Customer's request for Student Data in a student's records held by Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts Provider to review any of the Student Data accessed pursuant to the Services, Provider shall refer the parent or individual to Customer, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by Provider, Provider shall, at the request of Customer, transfer, or provide a mechanism for Customer to transfer, said Student-Generated Content to a separate 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 Provider pursuant to the Services, Provider shall notify Customer in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform Customer of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for Provider in order for Provider to provide the Services pursuant to this Addendum, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this Addendum.

ARTICLE III: DUTIES OF CUSTOMER

1. **Provide Data in Compliance with Applicable Laws**. Customer shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If Customer has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), Customer 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**. Customer 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**. Customer shall notify Provider promptly of any known unauthorized access. Customer will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. 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**" and/or otherwise authorized under the statutes referred to herein this Addendum or other applicable laws.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and subprocessors who have access to Student Data to comply with all applicable provisions of this Addendum with respect to the Student Data shared under the Addendum. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or subprocessor with access to Student Data pursuant to the Addendum.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any 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 Customer or this Addendum. 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 Provider pursuant to this Addendum. 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 Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the Customer or other governmental agencies in conducting research and other studies; and (2) research and development of Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this Addendum or any request by Customer to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior notice has been given to Customer of such disclosure. Prior to publishing any document that names the Customer explicitly or indirectly, Provider shall obtain the Customer's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data**. Upon written request from the Customer, Provider shall dispose of or provide a mechanism for the Customer to download or store Student Data obtained under this Addendum 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 Addendum, if no written request from the Customer is received, Provider shall dispose of all Student Data at the earliest of (a) Provider's standard destruction schedule; (b) when the Student Data is no longer needed for the purpose for which it was received; or (c) as otherwise required by law. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified.

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 Customer. 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 or Customer 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 Addendum 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 Customer, 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 Customer with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, Provider will allow the Customer 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 Customer . Provider will cooperate reasonably with the Customer and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of Provider and/or delivery of Services to students and/or Customer, and shall provide reasonable access to Provider's facilities, staff, agents and Customer's Student Data and all records pertaining to Provider, Customer and delivery of Services to the Customer. Failure to reasonably cooperate shall be deemed a material breach of the Addendum.

3. **Data Security**. Provider agrees to utilize adequate and appropriate administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification.

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 Provider Provider shall provide notification to Customer within 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 Provider and as it becomes available:

        i. The name and contact information of the reporting Customer 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; 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 Customer, upon request, with a summary of said written incident response plan.

(4) Customer shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from Customer's use of the Service, Provider shall cooperate with Customer to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this Addendum, they may do so by mutual written consent. Either party may terminate this Addendum and any service agreement or contract if the other party breaches any terms of this Addendum.

2. **Effect of Termination Survival**. If the Addendum is terminated, Provider shall destroy all of Customer's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements**. This Addendum 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 Addendum. This Addendum, together with any attachments, constitutes the entire Data Sharing Agreement between the Parties and supersedes all priopr agreements, understandings, and writings with respect to the subject matter hereof.

4. **Entire Agreement**. This Addendum, including all attachments, 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 Addendum may be amended and the observance of any provision of this Addendum 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 Addendum 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 Addendum, 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 Addendum or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction**. THIS ADDENDUM WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF COLORADO, 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 BOULDER COUNTY, COLORADO FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS ADDENDUM OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound**: This Addendum 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 In the event that Provider sells, merges, or otherwise disposes of its business to a successor during the term of this Addendum, Provider shall provide written notice to the Customer no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the Addendum and any obligations with respect to Student Data within the Addendum. The Customer has the authority to terminate the Addendum if it disapproves of the successor to whom Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this Addendum, 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 construed 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"

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.	X
	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 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)	
	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	

Category of Data	Elements	Check if Used by Your System
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	
	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 number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	X
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	
Student work	Student generated content; writing, pictures, etc.	X
	Other student work data -Please specify: *Content created from student prompts using generative artificial intelligence (AI) technology*	X
Transcript	Student course grades	
	Student course data	

Category of Data	Elements	Check if Used by Your System
	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 will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "B"
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 provided 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.

Metadata: means information that provides meaning and context to other 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 a Customer to provide a service to that Customer shall be considered an "operator" for the purposes of this section.

Provider: For purposes of the Addendum, 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 Addendum 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 Addendum 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 Lupin Learn Terms of Service.

Student Data: Student Data includes any data, whether gathered by Provider or provided by Customer 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 physical or 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, individual purchasing behavior or preferences, 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 Addendum, 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 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 Addendum, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than Customer or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

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 web site, 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 web site 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 Addendum, the term "Third Party" when used to indicate Provider of digital educational software or services is replaced by the term "Provider."