EDUCATIONAL AGENCY TERMS OF SERVICE

I. General Terms

A. These terms of service apply to any agreement between the parties for the provision of online products and/or services, software, or applications (including mobile applications - both of which are referred to as "apps") (referred to herein as the "Agreement"), and to use of the products and/or services licensed by the Agreement, including use by all of the educational agency's users and employees, and to students and their parents.

B. To the extent any provision of the Agreement or any privacy policy or other terms of service applicable to the product(s) and/or services licensed to or otherwise provided to the educational agency are in conflict with, inconsistent with, or incompatible with the provisions of these Educational Agency Terms of Service ("EATOS"), the EATOS shall control and take precedence over or replace those provisions. Agreement terms that are supplemental to and consistent with the EATOS shall remain in full force and effect.

C. Any applicable privacy policy or terms of service that users, students, or their parent/guardian must agree to in order to access or use the products, software, online site, service, or app (such as "click wrap" or "click to accept" protocols) do not apply to those users except for those that are consistent with and/or supplemental to, and not inconsistent with, these EATOS. Any inconsistent or incompatible terms do not apply to these users.

D. These EATOS shall be interpreted under the laws of the state of California, notwithstanding anything to the contrary in the Agreement, privacy policy, or other terms of service.

II. Definitions

A. The term "Agency" means the educational agency contracting with the operator(or licensor) of software or an online website, service, or app, and may also be referred to as Licensee.

B. The term "Consumer" means any individual who seeks or acquires, by purchase or lease, any goods, services, money, or credit for personal, family, or household purposes.

C. The term "Data" includes all "personally identifiable information," all pupil-generated content, and all other non-public information pertaining to any user, or to the parent or guardian of any pupil, obtained through use of the Operator's software, online site, service, or app.

D. The term "K-12 school purposes" means purposes that customarily take place at the direction of the K–12 school, teacher, or school district or aid in administration of school activities,

including but not limited to instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school and represent the intent of the Agency in entering into the Agreement.

E. The term "Operator" means the person or firm contracting to provide for Agency one or more products or services in connection with Operator's website, online service, or app. Operator may also be referred to as Licensor or Owner or Vendor.

F. The terms "personally identifiable information" or "PII" include but are not limited to student data, metadata, and user or pupil-generated content obtained by reason of the use of Operator's software, website, service, or app, including mobile apps, whether gathered by Operator or provided by Licensor or its users, students, or students' parents/guardians, and includes, without limitation, at least the following:

Information in the Student's Educational Record
Information in the Student's Email

First and Last Name
Telephone Number
Discipline Records
Special Education Data
Grades
Criminal Records
Health Records
Biometric Information
Socioeconomic Information
Political Affiliations
Text Messages
Student Identifiers
Photos
Geolocation Information

Home Address
Email Address
Test Results
Juvenile Dependency Records
Evaluations
Medical Records
Social Security Number
Disabilities
Food Purchases
Religious Information
Documents
Search Activity
Voice Recordings

Any Other Information that Allows Physical or Online Contact

Other Information that, Alone or in Combination, is Linked or Linkable to a Specific Student that Would Allow a Reasonable Person in the School Community, Who Does Not have Personal Knowledge of the Relevant Circumstances, to Identify the Student with Reasonable Certainty

Information Requested by a Person Who the Educational Agency or Institution Reasonably Believes Knows the Identity of the Student to Whom the Education Record Relates

G. The term “pupil-generated content” means materials created by a pupil, including but not limited to essays, research reports, portfolios, creative writing, music or other audio files, photographs, and account information that enables ongoing ownership of pupil content. "Pupil-generated content" does not include pupil responses to a standardized assessment where pupil possession and control would jeopardize the validity and reliability of that assessment.

H. The term “de-identified Data” means Data with all direct and indirect personal identifiers removed, including but not limited to all PII and school ID numbering, as well as any other sensitive and non-sensitive information that, alone or combined with other information that is linked or linkable to a specific individual, would allow identification.

III. Data De-identification/Re-identification

A. Licensor may use de-identified Data for product development, research, or other purposes.

B. Licensor agrees not to attempt to re-identify any de-identified Data and not to transfer or allow access to Data, including de-identified Data, to any party unless that party agrees not to attempt re-identification, including re-identification in connection with other Data available to that party from independent sources, even if publicly available.

IV. Mining, Marketing, and Advertising

A. Licensor is prohibited from mining Data for any purposes other than those K-12 school purposes agreed to by the parties. Data mining, collecting, or scanning user content or PII for the purpose of targeted advertising or marketing to students or their parents is prohibited.

B. Licensor will not use any Data, including de-identified Data, to advertise or market to pupils or their parents/guardians. Licensor will not perform any advertising or allow others to provide advertising to pupils or parents/guardians without the express written consent of Licensee.

C. To the extent any advertising is allowed, it must comply with California Business and Professions Code Section 22580 and will not include any of the prohibited products or services referenced in that section.

D. Advertising or marketing may be directed to Licensee only if student information is properly de-identified, unless the advertising is part of the express K-12 school purposes identified in the Agreement.

E. Operator is placed on notice that Licensee has not complied with all aspects of California Education Code Section 35182.5(c)(3) requiring that certain steps be taken before

Licensee enters into a contract that requires dissemination of advertising to pupils. Should Operator intend to submit any permitted advertising to pupils, Operator will first give Agency notice in writing of that intent and provide a reasonable opportunity for Agency to comply with all legal requirements.

F. California Education Code Section 35182.5(c)(3)(D) requires Licensee to afford parents/guardians an opportunity to opt out of receiving any advertising. Licensee will notify Licensor of those requests and Licensor will not submit, show, or display any advertising, whether targeted or general, to the identified students.

V. Licensor Collection and Use of Data

Licensor will only collect Data necessary to fulfill its duties as outlined in the Agreement. Licensor will use Data only for the purpose of fulfilling its duties and providing services under the Agreement, and for improving services under the Agreement. De-identified Data may be used as permitted in these EATOS.

VI. Data Sharing

Licensee understands that Licensor may rely on one or more subcontractors to perform various services under the Agreement. Licensor agrees to share the names of any subcontractors with Agency upon request. All subcontractors and successor entities of Licensor will be subject to the terms of the Agreement and these EATOS. Except as allowed in these EATOS, Data cannot be shared with any additional parties without prior written consent of the Agency, prior written consent of the parent/guardian of any minor pupil, or written consent of a pupil over the age of 18, except as required by law.

VII. Modification of Terms of Service

Licensor will not change how Data is collected, used, or shared under the terms of the Agreement in any way without advance notice to and written consent from Licensee. Any changes remain subject to these EATOS.

VIII. Data Transfer or Destruction

Licensor will ensure that all Data in its possession, and in the possession of any subcontractors or agents to which the Licensor may have transferred Data, is destroyed or transferred to Licensee under the direction of Licensee when the Data is no longer needed for its specified purpose, at the request of Licensee.

IX. Rights and License In and To the Data

A. The parties agree that all rights, including all intellectual property rights in and to pupil-generated content, are held by pupils and that all other rights to Data shall remain the exclusive property of Licensee; Licensor has a limited, nonexclusive license solely for the purpose of performing its obligations as outlined in the Agreement. The Agreement does not give Licensor any rights, implied or otherwise, to Data, pupil-generated content, or intellectual property, except as expressly stated in these EATOS; nor is this term to be interpreted to grant to anyone any rights in or to Licensor's software, online website, service, or app, including mobile apps, except as expressly stated in the Agreement.

B. Licensee's pupils may retain possession and control of their own pupil-generated content, if applicable, and may transfer pupil-generated content to a personal account by submitting a request through Licensee. Licensor shall facilitate that retention and/or transfer on request.

X. Access

Any Data (or any Data limited by identified user) held by Licensor will be made available to Licensee, and Licensee's designees (including students, parents, and guardians) upon request by Licensee.

XI. Security Controls

A. Licensor will store and process Data in accordance with industry best practices, to include appropriate administrative, physical, and technical safeguards to secure Data from unauthorized access, disclosure, and use. Licensor will conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner.

B. Licensor will have a written incident response plan, to include prompt notification of Licensee in the event of a security or privacy incident, as well as best practices for responding to a breach of PII. Licensor agrees to share its incident response plan upon request. Licensor's employees and subcontractors shall be trained in these procedures and practices at least annually. Compliance with this requirement shall not, in itself, absolve Licensor or any third party of liability in the event of an unauthorized disclosure of pupil records.

C. In the event of a breach of Licensor's data security, upon notice by Licensor, Licensee will notify eligible students, or the parents/guardians of minor students, of the breach following its policy and procedures, to include the following in which Licensor shall cooperate and provide any and all required information:

1. The security breach notification shall be written in plain language.

2. At a minimum, the security breach notification shall include the following:

a) Name and contact information of the reporting agency.

b) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

c) If the information is possible to determine at the time the notice is provided, then any of the following: (i) date of the breach, (ii) estimated date of the breach, or (iii) date range within which the breach occurred. The notification shall also include the date of the notice.

d) 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.

e) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

f) Toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

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

a) Information about what Licensee has done to protect individuals whose information has been breached.

b) Advice on steps that the person whose information has been breached may take to protect himself or herself.

4. The notice shall be given in a manner complying with the requirements of California Civil Code Section 1798.29.

5. If, pursuant to this section, Licensee is required to issue a security breach notification to more than 500 California residents as a result of a single breach of the security system, Licensee shall electronically submit a single sample copy of that security breach notification, excluding any PII, to the Attorney General.

XII. Do Not Track Instructions

Operator will permit users of its website, online service, or app to select a "do not track" or similar option to apply to their use, to the extent they are a "consumer" under these EATOS, unless tracking is an essential component of the K-12 school purposes stated in the Agreement.

XIII. Additional Requirements

A. The following additional requirements apply to an operator that has actual knowledge that the online site, service, or app is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes.

B. Operator shall not knowingly engage in any of the following activities with respect to its website, online service, or app:

1. Engage in targeted advertising on its website, online service, or app, or target advertising on any other site, service, or app, when the targeting of the advertising is based on any information (including covered information and persistent unique identifiers) that Operator has acquired through use of Operator's site, service, or app described in Paragraph A, above.

2. Use information (including persistent unique identifiers) created or gathered by Operator's website, online service, or app to amass a profile about a K–12 student except in furtherance of K–12 school purposes.

3. Sell a student's information (including covered information). This prohibition does not apply to the purchase, merger, or other type of acquisition of an Operator by another entity, provided that the Operator or successor entity continues to be subject to the provisions of this section with respect to previously acquired student information.

4. Disclose covered information unless the disclosure is made:

a) In furtherance of the K–12 purpose of the website, online service, or app, provided the recipient of the covered information disclosed pursuant to this paragraph:

(1) Shall not further disclose the information unless done to allow or improve operability and functionality within that student's classroom or school; and

(2) Is legally required to comply with Paragraph 4.D, above.

b) To ensure legal and regulatory compliance;

c) To respond to or participate in judicial process;

d) To protect the safety of users or others or security of the website; or

e) To a service provider, provided Operator contractually (i) prohibits the service provider from using any covered information for any purpose other than providing the contracted service to, or on behalf of, Operator, (ii) prohibits the service provider from disclosing any covered information provided by Operator to others, and (iii) requires the service provider to implement and maintain reasonable security procedures and practices as provided in Paragraph 4.D, above.

C. Nothing in Paragraph 4.B prohibits Operator's use of information for maintaining, developing, supporting, improving, or diagnosing Operator's website, online service, or app.

D. Operator shall:

1. Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information, and protect that information from unauthorized access, destruction, use, modification, or disclosure.

2. Delete a student's covered information if the school or district requests deletion of data under the control of the school or district.

E. Notwithstanding Paragraph 4.B., Operator may disclose a student's covered information as long as Items (1) to (3), inclusive, of that paragraph are not violated, under the following circumstances:

1. If other provisions of federal or state law require Operator to disclose the information and Operator complies with those requirements in protecting and disclosing that information.

2. For legitimate research purposes: (A) as required by state or federal law and subject to the restrictions under applicable laws, or (B) as allowed by state or federal law and under the direction of a school, school district, or state department of education, if no covered information is used for any purpose in furtherance of advertising or to amass a profile of the student for purposes other than K–12 school purposes.

3. To a state or local educational agency, including schools and school districts, for K–12 school purposes, as permitted by state or federal law.

F. Nothing in these additional requirements prohibits Operator from using de-identified student covered information as follows:

1. Within Operator's website, online service, or app, or other sites, services, or apps owned by Operator, to improve educational products.

2. To demonstrate the effectiveness of Operator's products or services, including in their marketing.

G. Nothing in these additional requirements prohibits Operator from sharing aggregated de-identified student covered information for development and improvement of educational websites, online services, or apps.

H. "Online service" includes cloud computing services, which must comply with these requirements if they otherwise meet the definition of an operator.

I. "Covered information" means personally identifiable information or materials in any media or format that are:

1. Created or provided by a student, or student's parent or legal guardian, to Operator in the course of the student's, parent's, or legal guardian's use of Operator's website, online service, or app for K–12 school purposes.

2. Created or provided by an employee or agent of the K–12 school, school district, local education agency, or county office of education, to Operator.

3. Gathered by Operator through operation of a website, online service, or app described in Paragraph A and descriptive of a student or otherwise identifying a 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 that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

J. These additional requirements shall not be construed to limit the authority of a law enforcement agency to obtain any content or information from Operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

K. These additional requirements do not limit Operator's ability to use student data (including covered information) for adaptive learning or customized student learning purposes.

L. These additional requirements do not apply to general audience websites, general audience online services, general audience online apps, or general audience mobile apps, even if login credentials created for Operator's website, online service, or app may be used to access those general audience sites, services, or apps

M. These additional requirements do not limit Internet service providers from providing Internet connectivity to schools or students and their families.

N. These additional requirements shall not be construed to prohibit Operator from marketing educational products directly to parents so long as the marketing did not result from use of covered information obtained by Operator through provision of services for K-12 school purposes.

O. These additional requirements do not impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or apps to review or enforce compliance of these requirements on those apps or software.

P. These additional requirements do not impose a duty upon a provider of an interactive computer service (as defined in Section 230 of Title 47 of the United States Code) to review or enforce compliance with these requirements by third party content providers.

Q. These additional requirements do not impede the ability of students to download, export, or otherwise save or maintain their own student created data or documents.

XIV. FERPA Compliance

The parties agree that when followed, these EATOS ensure compliance with the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g).