STANDARD STUDENT DATA PRIVACY AGREEMENT

NEW YORK

NY-DPA Modified Version 1.0

Erie 1 Board of Cooperative Educational Services (Erie 1 BOCES)

and

KHAN ACADEMY, INC.

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Erie 1 BOCES, located at 355 Harlem Road, West Seneca, NY 14224 (the "**Local Education Agency**" or "**LEA**") and Khan Academy, Inc., located in Mountain View, CA, with a postal address of P.O. Box 1630, Mountain View, CA 94042 (the "**Provider**"). Provider and LEA may collectively be referred to herein as the "Parties" or individually as a "Party."

WHEREAS, the Provider is providing educational or digital services to LEA.

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

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

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   √ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   √ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms.

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three years from July 1, 2025 through June 30, 2028. Exhibit E will expire (3) three years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices**. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Jason Hovey

Title: Director, School Partnerships

Address: P.O. Box 1630, Mountain View, CA 94042

Email: districts@khanacademy.org, with a copy to notices@khanacademy.org

The designated representative for the LEA for this DPA is:

Michelle Okal-Frink, Director of Instructional Technology, Research & Innovation
355 Harlem Road, West Seneca, NY 14224
Email: mokal@e1b.org
Phone: 716-821-7200

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

ERIE 1 BOCES

By: James Fregelette
Date: Jul 6, 2025

Printed Name: Jim Fregelette
Title/Position: Executive Director

KHAN ACADEMY, INC.

By: Julian Roberts
Date: 06/26/2025

Printed Name: Julian Roberts
Title/Position: Chief Financial Officer

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall 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 above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to 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 Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above. The student (or their parent) will be able to retain the student account and Learning Activity as described in Article II, Section 3 and Article IV, Section 6. For the purposes of this DPA, parent refers to the parent or legal guardian of the student.

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information. Notwithstanding the foregoing, Provider may provide direct assistance to the parent relating to parent accounts, and parents may view (but not modify or delete) information in the student's account.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider may, at the request of the LEA, student, or student's parent, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a personal account on Khan Academy, or otherwise enabling ongoing personal access through a Personal Login. In addition, prior to disposition of the student account in connection with the disposition of data under Article IV, Section 6, Provider may enable students or their parents to transfer Student Generated Content to a personal account on the Website or create a Personal Login to enable ongoing access. The transfer process may be accomplished as provided in this paragraph or as otherwise agreed between the Provider and the LEA. Prior to disposition of the student account, Provider may inform the student or the student's parent of the planned disposition of the account and options for retaining the Student Generated Content in a personal account. The student (if an eligible student) or their parent will be asked to confirm that they wish to maintain the account for personal use by providing their consent or instruction to maintain the account. In each case, requirements relating to transfer of data will be satisfied by transfer to a personal Khan Academy account or establishing a Personal Login credential to allow the student to maintain their account, and the mechanism for transfer may be accomplished by adding a Personal Login rather than creating a separate account.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

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

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining 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 the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time, applicable to Provider in providing the Services to LEA. For the purposes of this DPA, state and local laws, rules, and regulations are those identified in Exhibit "G."

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA or applicable law.

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

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of 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 LEA or this DPA. This prohibition against disclosure shall not apply to De-Identified Data, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, Subprocessors performing services on behalf of the Provider pursuant to this DPA, or authorized users of the Services (including students and parents using the intended functionality of the Services). For clarity, permitted disclosures to Subprocesses or pursuant to legal process include security consultants and law enforcement personnel made to protect the security of the Services. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA or the regulations referenced in Exhibit G and the following purposes: (1) conducting or assisting the LEA or other governmental agencies in conducting research and other studies; (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purposes and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer De-Identified Student Data (excluding aggregate summary data) to any third party unless that party agrees in writing not to attempt re-identification. Prior to publicly publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented, provided that this provision shall not apply to Provider's publication of aggregated, anonymized usage data. Provider may share De-identified Student Data with third party researchers for non-commercial educational research purposes, including efficacy research relating to Provider's educational sites, services, or applications and research of an academic or educational nature, *provided,* that third party researchers are bound by data sharing agreements that require the researcher to agree to confidentiality, privacy, restrictions on use and deletion of data consistent with the terms of this Agreement, and

commitments not to attempt re- dentification. Upon request by the LEA, the Provider will provide a list of third-party researchers that have access to De-Identified Student Data for research purposes, and will assist the LEA with questions relating to compliance with applicable law and data protection. The list of third-party researchers can also be found at this link. The LEA may opt out of data sharing with third party researchers for purposes unrelated to Provider's educational sites, services, or applications by providing notice of its election to opt out of data sharing to Provider's representative listed in this Agreement, with a copy to privacy@khanacademy.org.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement within 120 days of the date of said request (or such shorter period as is required under state law), and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of the Khan Academy Districts subscription, the LEA will provide written instruction to Provider to regarding disposition or transfer of student accounts and associated Student Data. Prior to receipt of a written instruction from the LEA, Provider will permit individual student accounts to remain open and available for use for other educational purposes. Provider shall dispose of all Student Data at the earliest of (a) Provider's standard destruction schedule, if applicable, provided the Student Data is no longer needed for the purpose for which it was received; or (b) as otherwise required by law. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account or made available through a Personal Login pursuant to Article II, Section 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either Party prior to the disposition of Student Data described in Exhibit "D." Requirements relating to transfer of data will be satisfied by transfer to a personal Khan Academy account or establishing a Personal Login credential to allow the student to maintain their account.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits. This section does not prohibit Provider from communicating with users generally via the Services or by sending Program Communications to users, or otherwise restrict Provider's activities relating to personal accounts. "Program Communications" means in-app or emailed communications relating to the educational Services, including prompts, messages and content relating to the use of the Services, for example; onboarding and orientation communications, recommendations for use of the Services, prompts for students to complete, or teachers to assign exercises or provide feedback as part of the learning exercise, periodic activity reports, suggestions for additional learning activities in the Services, service updates, and information about special or additional programs offered through the Services or offered to complement the programs offered through the Services.

ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** The Provider will cooperate reasonably with the LEA in responding to any state, or federal agency with oversight authority or jurisdiction over the LEA in connection with any audit or investigation of the LEA related to the LEA and/or delivery of Provider's Services to students and/or the LEA, and in connection with such audit shall provide reasonable access to the Provider's staff, agents and LEA's Student Data and records pertaining to the Provider and delivery of Services to the LEA. At least annually, Provider will obtain a Service Organization Controls (SOC) 2 Type II audit, or other commercially reasonable security audit, which attests to Provider's security policies, procedures, and controls, and which is performed by an independent third party based on recognized industry standards. Provider will make results of such controls review or audit available to LEA upon request and will address noted exceptions**.**

3. **Data Security**. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seven (7) days of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

   (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

      i. The name and contact information of the reporting LEA subject to this section.
      ii. A list of the types of personal information that were or are reasonably believed to have been the subject of 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 LEA, upon request, with a summary of said written incident response plan.

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

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

(6) This Section (Art. V, Sec. 4) shall not restrict Provider's ability to provide separate breach notification to its users with personal accounts.

ARTICLE VI: GENERAL OFFER OF 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 **Exhibit "E"** 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. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either Party may terminate this DPA and any Service Agreement if the other Party breaches any terms of this DPA.

2. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall dispose of or provide a mechanism for the transfer of Student Data as provided in Article IV, section 6. The LEA shall notify Provider when the Student Data it has provided pursuant to the DPA is no longer needed for the LEA's purpose(s) under the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will dispose of or transfer Student Data as set forth in Article IV, Section 6 (Disposition of Data).

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Updates to Schedules**. Provider may elect to amend Exhibits "A" and "B" to reflect changes in products

or services that result in new or enhanced features or capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed by providing an Addendum to this DPA. The Provider must notify the LEA and Subscribing LEAs, in accordance with the notification provisions of this DPA, of the existence and contents of an Addendum modifying Exhibit "A", "B" as applicable. The LEA or Subscribing LEA will have thirty (30) days from receipt to object to the Addendum. If no written objection is received it will become incorporated into the DPA between the parties.

5. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

6. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

7. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, 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 OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

8. **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 In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA 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 DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

9. **Authority.** Each Party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

10. **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"

DESCRIPTION OF SERVICES

This DPA applies to the use of Khan Academy Districts service (the "**District Service**") through School Accounts created by or at the direction of the LEA and which is provided pursuant to the Khan Academy Districts Terms of Service and entered into through execution of an order form between the LEA and Khan Academy (collectively, the order form and Khan Academy Districts Terms of Service form the "**Service Agreement**"). School Accounts are defined in, and must be established in accordance with, the Terms of Service. The District Service is a premium, subscription-based service that is offered as a complement to Khan Academy's website located at http://khanacademy.org and related mobile applications and online services (the "**Website**"), through which it provides educational services, including, but not limited to, educational content, and other products and services that Khan Academy may provide now or in the future. The District Service may include Khanmigo (an AI-powered educational guide with interactive activities and chat functionality) and AI-enabled tools.

Access to the Website and use of the standard features is provided free of charge, and is governed by and further described in Khan Academy's Terms of Service and Privacy Policy. Each student, teacher, and other LEA personnel enrolled in the District Service is registered with an individual user account on the Website. Website features:

- allow teachers and coaches to assign lessons to learners and monitor learning progress
- allow students to complete assignments or pursue independent learning
- permit users to connect their account to other authorized users who can view the account activity, including a parent or legal guardian ("**parent**"), or others as permitted by the intended functionality of the Services Website (this function may be limited to School Personnel included in the district's roster and parents at the request of the LEA)
- permit users to post or respond to questions relating to learning activities on the Website (this function may be disabled at the request of the LEA)
- offer additional educational programs (e.g., test prep, scholarship programs) through the Website
- in-app or emailed communications relating to the educational Services (Program Communications) that are not Targeted Advertising
- provide Program Communications relating to additional educational resources.

Khan Academy may engage in research studies or assist the LEA in conducting research and other studies at the request or direction of the LEA.

Students or teachers may have personal accounts in addition to School Accounts and may associate their School Accounts with their personal accounts. Additionally, they may choose to create personal login information to their School Account to provide access to the account for activity outside of school ("**Personal Login**"). Parents may elect to create a personal account on the Website associated with their child's account and monitor their child's learning activity. This DPA does not apply to personal accounts (or information users provide to Khan Academy through such personal accounts). Khan Academy may provide direct assistance to students and their parents requesting access to information in the student's Khan Academy account. Personal account activity is governed by Provider's Website Terms of Service and Privacy Policy.

In addition to the District Services for School Accounts covered by this DPA, Khan Academy allows users to create free Website accounts, and offers supplemental services to school districts and educational agencies to facilitate implementation by the district or agency. These supplemental services are provided under separate terms of service and data protection terms that address the specific features and use of data for those services. This DPA does not apply to Khan Academy Kids mobile application, Khan Academy Kids Classroom Service, or MAP Accelerator services.

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: *Khan Academy may obtain access to standardized test scores in order to create a personalized learning plan.*	✓
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 (optional)	✓
	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: *Teachers may choose to identify the school. Grade level information may be provided or inferred from subjects studied.*	✓
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 (school email only)	✓
	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 (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.	✓
	Other student work data -Please specify: *Information about use of the Website and activities on the Website, including use and engagement with Khanmigo.*	✓
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	

Category of Data	Elements	Check if Used by Your System
	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:	

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and 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 an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

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

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content. Student Generated Content includes Learning Activity. "Learning Activity" means information relating to an identified student's use of the Website generated by the user through use of the Website.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose in connection with the Services, 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 that is associated with an identified individual. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not include De-Identified Data or information that has been anonymized, or anonymous usage data regarding a student's use of Provider's services.

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

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet 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 DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

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

1. Extent of Disposition

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

[**Insert categories of data here**]

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

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

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

[**Insert or attach special instructions**]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [**Insert Date**]

4. Signature

____ ______________

Authorized Representative of LEA Date

5. Verification of Disposition of Data

____ ______________

Authorized Representative of Company 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 Erie 1 BOCES ("Originating LEA") which is dated Jul 6, 2025, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("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 Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form.

Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following **email address:** ____.

KHAN ACADEMY, INC.

BY: Julian Roberts Date: 06/27/2025

Printed Name: Julian Roberts Title/Position: CFO

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 for the term of the DPA between the Erie 1 BOCES and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

Subscribing LEA: (School District Name): ______________________________

BY: ______________________________ Date: ______________________________

Printed Name: ______________________________ Title/Position: ______________________________

DESIGNATED REPRESENTATIVE OF LEA:

Name: ______________________________

Title: ______________________________

Address: ______________________________

Telephone Number: ______________________________

Email: ______________________________

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

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

Cybersecurity Frameworks

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

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

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

Exhibit "G"
New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

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

1. All employees of the Provider who will have direct (in person or otherwise unmonitored) contact with students shall pass criminal background checks. Unless otherwise agreed between the Parties, Provider's services will be provided online only.

2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA and as expressly permitted in this DPA.

3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy as applicable to the nature of the Services. For clarity and with respect to LEA's Data Security and Privacy Policy (and any other document provided by LEA including the Parents Bill of Rights for Data Security and Privacy) (collectively "**LEA Policies**"), the terms of this DPA shall be deemed in compliance, and Provider shall not be required to comply with the LEA Policies to the extent (i) they are inapplicable to the nature of the Services; or (ii) Vendor is not afforded an opportunity to review, confirm compliance, and provide any clarifications. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations. Following execution of Exhibit "E", each Subscribing LEA will provide its Data Security Policy to the Provider for review. If the Provider does not notify the LEA of any objections to the Data Security and Privacy Plan within forty-five (45) days of the Provider's receipt of the same in writing, the Provider will adhere to that Data Security and Privacy Plan. If the Provider raises concerns, the Subscribing LEA and Provider will work together to resolve the concerns in good faith.

4. Provider represents that their Data Privacy and Security Plan can be found in Exhibit K which is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees, and contractually imposes substantially similar training requirements on its subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are

required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction. For clarity, local data privacy and security requirements refer to New York Education Law § 2-d in alignment with Section 3 herein.

5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to "Student Data" shall be amended to include and state, "Student Data and APPR Data."

7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply in all material respects with the LEA's Data Privacy and Security Policy as applicable to the Service and nature of the data processed. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

8. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement." Use of data authorized under the DPA is considered use for permitted purposes.

9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained, in accordance with Paragraph 4 above, on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider's employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.

10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or

placed in a separate student account or made available through a Personal Login pursuant to Article II, Section 3. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying that it and it's subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.

Upon termination of the applicable Service Agreement, if no written request from the LEA is received, Provider shall automatically dispose of all student data and Student Accounts after one hundred twenty days (120) days. The Provider agrees that the timelines for disposition of data will be modified by any subsequent instruction by the LEA to retain student accounts, which will control in the case of a conflict. Further, if either Party seeks to terminate this DPA, they may do so by terminating the Service Agreement (subject to LEA and Provider cooperating to ensure that all applicable Student Accounts governed by the Service Agreement have been transferred or deleted).

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account or made available through a Personal Login pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D",** or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **"Exhibit D".** Requirements relating to transfer of data will be satisfied by transfer to a personal Khan Academy account or establishing a Personal Login credential to allow the student to maintain their account.

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."

12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

13. To replace Article V, Section 2 (Audits) to state: The Provider will cooperate reasonably with the LEA in responding to any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider relating to delivery of Services to students and/or the LEA. In connection with such investigation, Provider shall provide reasonable access to (i) the Provider's staff and agents with knowledge of the subject data processing activity; (ii) LEA's Student Data and (iii) all records pertaining to the Provider reasonably relating to any such investigation, LEA and delivery of Services to the LEA as necessary to comply with applicable law.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require Contractor to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. For clarity, a Service Organization Controls (SOC) 2 Type II audit performed by an independent third party fulfills this industry standard independent audit. At least annually, Provider will obtain a Service Organization Controls (SOC) 2 Type II audit, or other commercially reasonable security audit, which attests to Provider's security policies, procedures, and controls, and which is performed by an independent third party based on recognized industry standards. Provider will make results of such controls review or audit available to LEA upon request and will address noted exceptions. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA in the most expedient way possible and without unreasonable delay but no more than seven (7) calendar days after discovery of such breach , unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

i. The name and contact information of the reporting LEA subject to this section.

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of 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; and

vi. The number of records affected, if known; and

vii. A description of the investigation or plan to investigate; and

viii. The name of a point of contact for representatives who can assist parents or eligible students that have additional questions.

(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 LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors and notice of Breach is required by applicable law, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals. This Section (Art. V, Sec. 4) shall not restrict Provider's ability to provide separate breach notification to its users with personal accounts.

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

(6) Provider will (and will request of its subprocessors to the extent such subprocessor has access to unencrypted Student Data) cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach as necessary to comply with law. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.
- "Provider" is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting. - **APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d

- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.

- **Disclose or Disclosure**: The intentional or unintentional communication, release, or transfer of Student

Data and/or APPR Data by any means, including oral, written, or electronic. - **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or

indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services (BOCES), then the term LEA shall also include Participating School Districts for purposes of the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.
- **Participating School District**: As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement (sometimes referred to as a component school district of a BOCES) with LEA, and shall include LEA if it uses the Services in its own educational or operational programs provided that if such LEA is a BOCES, the Provider is supplied with written notice of the component school districts procuring access through such BOCES.

Exhibit "J"

LEA Documents

New York LEAs will provide links to their Data Security and Privacy Policy, Parents Bill of Rights for Data Security and Privacy, and supplemental information for this service agreement in their Exhibit Es.

Erie 1 BOCES:

https://sdpc.a4l.org/ny_dp_bor_url.php?districtID=13045

Exhibit "K"

Provider Security Policy

DATA PRIVACY AND SECURITY PLAN UNDER NEW YORK EDUCATION LAW § 2-d

In accordance with New York Education Law § 2-d(5)(e), set forth below is Khan Academy's Data Security and Privacy Plan for Student Data obtained in the course of providing its Service for School use.

This Data Privacy and Data Security Plan outlines how Khan Academy will implement safeguards to protect the security and privacy of Student Data, consistent with the requirements of applicable law, including New York Education Law § 2-d, FERPA and COPPA.

Privacy

Khan Academy understands how important privacy is to our learners, their families and schools, and we are committed to creating a safe and secure environment for learners of all ages. Khan Academy's Privacy Policy informs users of Khan Academy's policies and procedures regarding the collection, use, and disclosure of their Personally Identifiable Information, Student Data, and De-Identified Data consistent with applicable federal and state laws. The Khan Academy Privacy Policy includes a section on Schools and student use, which details our privacy commitments specific to school users and student records.

Khan Academy maintains and follows policies and procedures designed to ensure compliance with U.S. federal and state laws applicable to its services. Customer shall provide Khan Academy with copies of any additional local or district specific privacy and data security policies that are applicable to the Services and provide Khan Academy with an opportunity to review and confirm its acceptance of such policies.

Teacher and Principal Data

Khan Academy does not collect Teacher or Principal Data, as defined in New York Education Law § 2-d, in the course of providing its services. Khan Academy's Services do not include providing performance reviews of classroom teachers or principals, and Khan Academy does not authorize the use of its Services for this purpose.

Administrative, Operational and Technical Safeguards for Sensitive Data

Khan Academy employs administrative, operational, and technical safeguards designed to ensure the appropriate security of Student Data, including protection from unauthorized access, disclosure, use or acquisition by an unauthorized person. These safeguards include:

Technical Safeguards

- *Encryption of data in transit*. Khan Academy employs industry standard encryption technology to protect information and data transmitted over the internet or other public networks.
- *Data storage and server hosting*. Khan Academy utilizes leading secure cloud service providers, and we rely on them for server and datacenter security. The website is hosted on the Google Cloud Platform (GCP). All data on GCP is encrypted at rest in accordance with Google's security practices.
- *Data access control*. Khan Academy uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources or user data. Asset owners are responsible for granting access based on the users' role, and access is reviewed periodically.

- *Software development lifecycle*. Khan Academy maintains documented software development lifecycle policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. We follow NIST and OWASP best practices and recommendations in the course of our product development.

Administrative Safeguards

- *Risk management*. Khan Academy employs a cross-functional risk management process to identify and manage strategic, operational and compliance risks. A variety of methods are used to assess and manage risk, including policies, procedures, and use of industry standard tools to monitor and protect data and systems.
- *Background checks*. Khan Academy employees are screened with background checks prior to their employment with us.
- *Employee use of equipment and tools*. Laptops issued to our employees for work purposes are managed to ensure that they are properly configured, regularly updated, and tracked. Our default configuration includes full-disk encryption of hard drives, on-device threat detection and reporting capabilities, and lock when idle for a specified amount of time. All laptops are securely wiped following NIST guidelines before we re-issue or dispose of them. All employees are required to use multi-factor authentication and strong passwords following NIST guidelines to access Khan Academy resources.
- *Vulnerability management*. Khan Academy uses a variety of tools, practices and procedures to monitor and protect our data and systems. Khan Academy maintains a confidential vulnerability disclosure program that fields reports from security researchers, and reports are promptly triaged, prioritized and addressed according to their severity.

Employee Training

Our employees are required to complete information security awareness training upon hire and periodically thereafter. Personnel are required to acknowledge and agree to our written information security policy and our employee handbook which, among other things, highlights our commitment to keep Student Data and confidential information secure. Additionally, employees that have access to Student Data receive training on applicable federal and state privacy laws.

Third-Party Service Providers; Vendor Management

In order to provide its services, Khan Academy may engage third parties to provide services, such as server and data hosting, email delivery, customer service support, analytics, and communication tools and services. We review third-party service provider security controls, privacy and data protection policies, and contract terms upon initial engagement and periodically thereafter. Third-party service providers are required to enter into written agreements whereby they agree to protect the security, privacy and confidentiality of Student Data. Third-party service providers are prohibited from engaging in targeting advertising and any other use of Student Data except in support of the services we provide to the customer.

Incident Management

Khan Academy maintains an incident management process for data security and privacy incidents that may affect the confidentiality, integrity, or availability of systems or data. Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology and security incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents.

Khan Academy's incident response procedures include procedures to provide prompt notification regarding security breaches in accordance with applicable state law or without unreasonable delay, whichever occurs sooner, including a description of the security breach based on available information, and contact information for the Khan Academy representative(s) who will be available to assist the subscribing school district. Khan Academy may concurrently provide breach notifications to its customers, including parents and other individuals with website accounts.

Rectification & Access Student Data

Users or parents of such users (if a user is a minor) may review and amend Student Data of such user by contacting the subscribing school district and following the subscribing school district's procedures for amending such user's Student Data. During the term of a paid subscription, administrative controls for accounts used in a school setting, including the ability to modify or delete the account, are held by the school subscriber and Khan Academy will not make any changes to any student education records without the applicable subscribing school district's express written permission, and then, only in accordance with applicable law. At the expiration of the paid subscription term, students over the age of 13, or parents associated with an account for a child under 13 years of age are able to modify or delete the account.

With respect to requests to view or obtain copies of student Personally Identifiable Information in the district's School Accounts maintained by Khan Academy, students can access the data in their account profile directly. In addition, parents may elect to open a free parent account associated with their student's account on the Website and will be able to view the student's account profile information and view their account activity through the parent account. Khan Academy may directly assist the parent or guardian with respect to their request to establish a parent account. Parent accounts are personal accounts established by the parent and are not part of the Services provided to the district by Khan Academy.

Data Retention, Destruction & Return of Student Data

Khan Academy will retain Student Data for the length of time necessary to meet our contractual and legal commitments under subscription agreements entered into with the district. Khan Academy's Services do not include storage or maintenance of Student Data after the expiration of the subscription term for paid services. Data in student accounts are considered duplicate records or similar data having a retention period of 0 after needed. The district is responsible for submitting a deletion request (pursuant to the process agreed upon in the respective contract) for accounts that are no longer needed for an educational purpose.

Student-generated content (if any) is not severable from the Services. Any requirements relating to transfer to a separate account will be satisfied through establishing a personal Khan Academy account or login credential to retain the content.

Upon deletion of School Account, Student Data received by Khan Academy will be either: (a) retained in a personal account as directed by the Parent or Legal Guardian or Student; (b) de-identified; or (c) deleted from Khan Academy's computer systems. Khan Academy retains De-Identified Data indefinitely for purposes stated in its Privacy Policy. Information is considered to be de-identified when all Personally Identifiable Information, including indirect identifiers, has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, and includes aggregated usage data. Indirect identifiers mean any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty.

KAD DPA_ NY_With_NY_LEA_Info_Added-2

Final Audit Report 2025-06-26

Created:	2025-06-26
By:	Danielle Sullivan (daniellesullivan@khanacademy.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAMeo1h7FwFWQS-ilzdgGJ_R3Aa84vD8Bk

"KAD DPA_ NY_With_NY_LEA_Info_Added-2" History

Document created by Danielle Sullivan (daniellesullivan@khanacademy.org)
2025-06-26 - 11:25:22 PM GMT

Document emailed to Jullian Roberts (julian@khanacademy.org) for signature
2025-06-26 - 11:26:25 PM GMT

Email viewed by Jullian Roberts (julian@khanacademy.org)
2025-06-26 - 11:40:05 PM GMT

Document e-signed by Jullian Roberts (julian@khanacademy.org)
Signature Date: 2025-06-26 - 11:40:29 PM GMT - Time Source: server

✓ Agreement completed.
2025-06-26 - 11:40:29 PM GMT

KAD DPA_ NY_With_NY_LEA_Info_Added-2 - KA signed

Final Audit Report 2025-06-27

Created:	2025-06-27
By:	Danielle Sullivan (daniellesullivan@khanacademy.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAAIMFD2UaXoxHs1rX-TmsqtF-C0ZuNIwo2

"KAD DPA_ NY_With_NY_LEA_Info_Added-2 - KA signed" History

Document created by Danielle Sullivan (daniellesullivan@khanacademy.org)

2025-06-27 - 4:29:04 PM GMT

Document emailed to Julian Roberts (julian@khanacademy.org) for signature

2025-06-27 - 4:30:58 PM GMT

Email viewed by Julian Roberts (julian@khanacademy.org)

2025-06-27 - 5:10:26 PM GMT

Document e-signed by Julian Roberts (julian@khanacademy.org)

Signature Date: 2025-06-27 - 5:10:54 PM GMT - Time Source: server

✓ Agreement completed.

2025-06-27 - 5:10:54 PM GMT

KhanAcademy_ NY_VendorSigned

Final Audit Report 2025-07-07

Created:	2025-06-27
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA3SwVNgqBPVVuBwi1X9E3rqG0dGAt48tu

"KhanAcademy_ NY_VendorSigned" History

Document created by Ramah Hawley (rhawley@tec-coop.org)
2025-06-27 - 5:57:56 PM GMT

Document emailed to James Fregelette (jfregelette@e1b.org) for signature
2025-06-27 - 5:58:06 PM GMT

Email viewed by James Fregelette (jfregelette@e1b.org)
2025-06-27 - 8:19:52 PM GMT

Email viewed by James Fregelette (jfregelette@e1b.org)
2025-07-07 - 0:39:56 AM GMT

Document e-signed by James Fregelette (jfregelette@e1b.org)
Signature Date: 2025-07-07 - 0:45:10 AM GMT - Time Source: server

✓ Agreement completed.
2025-07-07 - 0:45:10 AM GMT

Exhibit "G"

New York

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New York. Specifically, those laws are New York Education Law § 2-d; and the Regulations of the Commissioner of Education at 8 NYCRR Part 121; and

WHEREAS, the Parties wish to enter into these additional terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New York;

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

1. All employees of the Provider who will have direct (in person or otherwise unmonitored) contact with students shall pass criminal background checks. Unless otherwise agreed between the Parties, Provider's services will be provided online only.

2. Student Data will be used by Provider exclusively to provide the Services identified in Exhibit A to the DPA~~.~~ and as expressly permitted in this DPA.

3. Provider agrees to maintain the confidentiality and security of Student Data in accordance with LEA's Data Security and Privacy Policy~~.~~ as applicable to the nature of the Services. For clarity and with respect to LEA's Data Security and Privacy Policy (and any other document provided by LEA including the Parents Bill of Rights for Data Security and Privacy) (collectively "**LEA Policies**"), the terms of this DPA shall be deemed in compliance, and Provider shall not be required to comply with the LEA Policies to the extent (i) they are inapplicable to the nature of the Services; or (ii) Vendor is not afforded an opportunity to review, confirm compliance, and provide any clarifications. The LEA's Data Security Policy is attached hereto as Exhibit J. Each Subscribing LEA will provide its Data Security Policy to the Provider upon execution of Exhibit "E". Provider shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect Student Data and APPR Data. Provider must Encrypt Student Data and APPR Data at rest and in transit in accordance with applicable New York laws and regulations. Following execution of Exhibit "E", each Subscribing LEA will provide its Data Security Policy to the Provider for review. If the Provider does not notify the LEA of any objections to the Data Security and Privacy Plan within forty-five (45) days of the Provider's receipt of the same in writing, the Provider will adhere to that Data Security and Privacy Plan. If the Provider raises concerns, the Subscribing LEA and Provider will work together to resolve the concerns in good faith.

4. Provider represents that their Data Privacy and Security Plan can be found ~~at the URL link listed~~ in Exhibit K ~~and~~which is incorporated into this DPA. Provider warrants that its Data Security and Privacy Plan, at a minimum: (a) implements all applicable state, federal and local data privacy and security requirements; (b) has operational technical safeguards and controls in place to protect PII that it will receive under the service agreement; (c) complies with the LEA's parents bill of rights for data privacy and security; (d) requires training of all providers' employees, assignees ~~and~~, and contractually imposes substantially similar training

requirements on its subprocessors who have Access to student data or APPR data; (e) ensures subprocessors are required to protect PII received under this service agreement; (f) specifies how data security and privacy incidents that implicate PII will be managed and ensuring prompt notification to the LEA, and (g) addresses Student Data return, deletion and destruction. For clarity, local data privacy and security requirements refer to New York Education Law § 2-d in alignment with Section 3 herein.

5. In addition to the requirements described in Paragraph 3 above, the Provider's Data Security and Privacy Plan shall be deemed to incorporate the LEA's Parents Bill of Rights for Data Security and Privacy, as found at the URL link identified in Exhibit J. The Subscribing LEA will provide its Parents Bill of Rights for Data Security and Privacy to the Provider upon execution of Exhibit "E".

6. All references in the DPA to "Student Data" shall be amended to include and state, "Student Data and APPR Data."

7. To amend Article II, Section 5 to add: Provider shall ensure that its subprocessors agree that they do not have any property, licensing or ownership rights or claims to Student Data or APPR data and that they will comply in all material respects with the LEA's Data Privacy and Security Policy as applicable to the Service and nature of the data processed. Provider shall examine the data privacy and security measures of its Subprocessors. If at any point a Subprocessor fails to materially comply with the requirements of this DPA, Provider shall: (i) notify LEA, (ii) as applicable, remove such Subprocessor's Access to Student Data and APPR Data; and (iii) as applicable, retrieve all Student Data and APPR Data received or stored by such Subprocessor and/or ensure that Student Data and APPR Data has been securely deleted or securely destroyed in accordance with this DPA. In the event there is an incident in which Student Data and APPR Data held, possessed, or stored by the Subprocessor is compromised, or unlawfully Accessed or disclosed, Provider shall follow the Data Breach reporting requirements set forth in the DPA.

8. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement." Use of data authorized under the DPA is considered use for permitted purposes.

9. To amend Article IV, Section 3 to add: Provider shall ensure that all its employees and subprocessors who have Access to or will receive Student Data and APPR Data will be trained, in accordance with Paragraph 4 above, on the federal and state laws governing confidentiality of such Student Data and APPR Data prior to receipt. Access to or Disclosure of Student Data and APPR Data shall only be provided to Provider's employees and subprocessors who need to know the Student Data and APPR Data to provide the services and such Access and/or Disclosure of Student Data and APPR Data shall be limited to the extent necessary to provide such services.

10. To replace Article IV, Section 6 (Disposition of Data) with the following: Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within ninety (90) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Provider is prohibited from retaining disclosed Student Data or continuing to Access Student Data beyond the term of the Service Agreement unless such retention is expressly authorized for a prescribed period by the Service Agreement, necessary for purposes of facilitating the transfer of disclosed Student Data to the LEA, or expressly required by law. The duty to

dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account or made available through a Personal Login pursuant to Article II, Section 3. The confidentiality and data security obligations of Provider under this DPA shall survive any termination of this contract to which this DPA is attached but shall terminate upon Provider's certifying that it and it's subprocessors, as applicable: (a) no longer have the ability to Access any Student Data provided to Provider pursuant to the Service Agreement and/or (b) have destroyed all Student Data and APPR Data provided to Provider pursuant to this DPA. The Provider agrees that the timelines for disposition of data will be modified by any Assurance of Discontinuation, which will control in the case of a conflict.
~~pursuant to~~
Upon termination of the applicable Service Agreement, if no written request from the LEA is received, Provider shall automatically dispose of all student data and~~/or (b) have destroyed all~~ Student ~~Data and APPR Data provided to Provider pursuant to this DPA.~~Accounts after one hundred twenty days (120) days. The Provider agrees that the timelines for disposition of data will be modified by any ~~assurance of discontinuation~~subsequent instruction by the LEA to retain student accounts, which will control in the case of a conflict. Further, if either Party seeks to terminate this DPA, they may do so by terminating the Service Agreement (subject to LEA and Provider cooperating to ensure that all applicable Student Accounts governed by the Service Agreement have been transferred or deleted).

~~Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all student data after providing the LEA with ninety (90) days prior notice.~~

The duty to dispose of student data shall not extend to Student Data that had been de-identified or placed in a separate student account or made available through a Personal Login pursuant to section II 3. The LEA may employ a "**Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D",** or, with reasonable notice to the Provider, other form of its choosing. No further written request or notice is required on the part of either party prior to the disposition of Student Data described in **"Exhibit D".** Requirements relating to transfer of data will be satisfied by transfer to a personal Khan Academy account or establishing a Personal Login credential to allow the student to maintain their account.

11. To amend Article IV, Section 7 to add: 'Notwithstanding the foregoing, Provider is prohibited from using Student Data or APPR data for any Commercial or Marketing Purpose as defined herein. And add after (iii) account holder, "which term shall not include students."

12. To replace Article V, Section 1 (Data Storage) to state: Student Data and APPR Data shall be stored within the United States and Canada only. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

~~1.~~ 13. To replace Article V, Section 2 (Audits) to state: ~~No more than once a year or following an unauthorized Access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA or its designee(s) to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA .~~ The Provider will cooperate reasonably with the LEA ~~or its designee(s) and~~in responding to any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider ~~and/or~~relating to delivery of Services to students and/or ~~LEA, and~~ the LEA. In connection with such investigation, Provider shall provide reasonable ~~Access~~access to (i) the Provider's

~~facilities,~~ staff~~,~~ and agents ~~and~~with knowledge of the subject data processing activity; (ii) LEA's Student Data and (iii) all records pertaining to the Provider reasonably relating to any such investigation, LEA and delivery of Services to the LEA~~.~~ as necessary to comply with applicable law.

Upon request by the New York State Education Department's Chief Privacy Officer (NYSED CPO), Provider shall provide the NYSED CPO with copies of its policies and related procedures that pertain to the protection of information. In addition, the NYSED CPO may require ~~Provider~~Contractor to undergo an audit of its privacy and security safeguards, measures, and controls as they pertain to alignment with the requirements of New York State laws and regulations, and alignment with the NIST Cybersecurity Framework. Any audit required by the NYSED CPO must be performed by an independent third party at Provider's expense and the audit report must be provided to the NYSED CPO. In lieu of being subject to a required audit, Provider may provide the NYSED CPO with an industry standard independent audit report of Provider's privacy and security practices that was issued no more than twelve months before ~~the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. Failure to~~ the date that the NYSED CPO informed Provider that it required Provider to undergo an audit. For clarity, a Service Organization Controls (SOC) 2 Type II audit performed by an independent third party fulfills this industry standard independent audit. At least annually, Provider will obtain a Service Organization Controls (SOC) 2 Type II audit, or other commercially reasonable security audit, which attests to Provider's security policies, procedures, and controls, and which is performed by an independent third party based on recognized industry standards. Provider will make results of such controls review or audit available to LEA upon request and will address noted exceptions. Failure to reasonably cooperate with any of the requirements in this provision shall be deemed a material breach of the DPA.

To amend the third sentence of Article V. Section 3 (Data Security) to read: The Provider shall implement security practices that are in alignment with the NIST Cybersecurity Framework v1.1 or any update to this Framework that is adopted by the New York State Department of Education.

14. To replace Article V. Section 4 (Data Breach) to state: In the event of a Breach as defined in 8 NYCRR Part 121.1 Provider shall provide notification to LEA ~~within seventy-two (72) hours of confirmation of~~in the ~~incident~~most expedient way possible and without unreasonable delay but no more than seven (7) calendar days after discovery of such breach , unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

i. The name and contact information of the reporting LEA subject to this section.

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of 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; and

vi. The number of records affected, if known; and

vii. A description of the investigation ~~undertaken so far~~or plan to investigate; and

viii. The name of a point of contact for ~~Provider.~~representatives who can assist parents or eligible students that have additional questions.

(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 LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians. Where a Breach of Student Data and/or APPR Data occurs that is attributable to Provider and/or its Subprocessors and notice of Breach is required by applicable law, Provider shall pay for or promptly reimburse LEA for the full cost of notification to Parents, Eligible Students, teachers, and/or principals. This Section (Art. V, Sec. 4) shall not restrict Provider's ability to provide separate breach notification to its users with personal accounts.

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

(6) Provider will (and will request of its subprocessors ~~will~~to the extent such subprocessor has access to unencrypted Student Data) cooperate with the LEA, the NYSED Chief Privacy Officer and law enforcement where necessary, in any investigations into a Breach~~.~~ as necessary to comply with law. Any costs incidental to the required cooperation or participation of the Provider will be the sole responsibility of the Provider if such Breach is attributable to Provider or its subprocessors.

15. To amend the definitions in Exhibit "C" as follows:

- "Subprocessor" is equivalent to subcontractor. It is a third party who the provider uses for data collection, analytics, storage, or other service to allow Provider to operate and/or improve its service, and who has access to Student Data.
- "Provider" is also known as third party contractor. It any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs. Such term shall include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities and is not an educational agency and a not-for-profit corporation or other non-profit organization, other than an educational agency.

16. To add to Exhibit "C" the following definitions:

- **Access:** The ability to view or otherwise obtain, but not copy or save, Student Data and/or APPR Data arising from the on-site use of an information system or from a personal meeting. - **APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d
- **Commercial or Marketing Purpose:** In accordance with § 121.1(c) of the regulations of the New York Commissioner of Education, the Disclosure, sale, or use of Student or APPR Data for the purpose of directly or indirectly receiving remuneration, including the Disclosure, sale, or use of Student Data or APPR Data for advertising purposes, or the Disclosure, sale, or use of Student Data to develop, improve, or market products or services to Students.
- **Disclose or Disclosure**: The intentional or unintentional communication, release, or transfer of Student Data and/or APPR Data by any means, including oral, written, or electronic. - **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 Security Rule at 45 CFR § 164.304, encrypt means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or

  indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
- **Release:** Shall have the same meaning as Disclose
- **LEA:** As used in this DPA and all Exhibits, the term LEA shall mean the educational agency, as defined in Education Law Section 2-d, that has executed the DPA; if the LEA is a board of cooperative educational services~~,~~ (BOCES), then the term LEA shall also include Participating School Districts for purposes of

the following provisions of the DPA: Article I, Section 2; Article II, Sections 1 and 3; and Sections 1, 2, and 3 of Article III.

- **Participating School District**: As used in Exhibit G and other Exhibits to the DPA, the term Participating School District shall mean a New York State educational agency, as that term is defined in Education Law Section 2-d, that obtains access to the Services through a CoSer agreement (sometimes referred to as a component school district of a BOCES) with LEA, and shall include LEA if it uses the Services in its own educational or operational programs~~.~~ provided that if such LEA is a BOCES, the Provider is supplied with written notice of the component school districts procuring access through such BOCES.