

**STUDENT DATA PRIVACY ADDENDUM**

**between**

**the LEA named herein**

**and**

**KHAN ACADEMY, INC., a 501(c)(3) organization**

**for use in**

**NEW YORK STATE**

**including**

**Parent's Bill of Rights (Exhibit E)**

**and**

**Supplemental Information (Exhibit F)**

This Student Data Privacy Addendum (“**DPA**”) is incorporated by reference into the Service Agreement (as defined in Exhibit C) entered into by and between the school district located solely within the United State set forth below (hereinafter referred to as “**LEA**”) and Khan Academy, Inc. (hereinafter referred to as “**Provider**”) effective as of the date the DPA is signed by both the LEA and the Provider (“**Effective Date**”).

**WHEREAS**, Provider is (or will be) providing educational or digital services to LEA under the terms set forth in the Service Agreement;

**WHEREAS**, Provider and LEA recognize the need to protect student Personally Identifiable Information and other regulated data exchanged between them as required by applicable United States 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), Protection of Pupil Rights Amendment (“**PPRA**”) 20 U.S.C. §§ 1400 et. seq., and applicable state privacy laws and regulations, including, but not limited to New York State Education Law § 2-d (“**Education Law § 2-d**”);

**WHEREAS**, in accordance with Education Law § 2-d(3)(c) and Section 121.3 of the implementing Regulations, the attached Exhibit “E” includes the Parents Bill of Rights for Data Privacy and Security and the attached Exhibit “F” includes the “Supplemental Information” required to be posted on the LEA’s website; and

**WHEREAS**, 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. This DPA describes the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to such Student Data.
2. The services to be provided by Provider to LEA pursuant to this DPA are detailed in Exhibit “A” (the “**Services**”).
3. 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:

**For Khan Academy website, mobile application and related services:**

Jason Hovey, Director of School Partnerships  
Khan Academy, Inc.  
P.O. Box 1630, Mountain View, CA 94042  
[schoolpartnerships@khanacademy.org](mailto:schoolpartnerships@khanacademy.org)

All legal notices shall also be sent by email to [notices@khanacademy.org](mailto:notices@khanacademy.org).

The designated representative for the LEA for this DPA is:

Name: Brian Zolnowski  
Title: Data Protection Officer  
Address: 2045 School St. North Collins, NY 14111  
Email: DPO@northcollinscsd.org

LEA's contact for parent inquiries:

Name: Brian Zolnowski  
Title: Data Protection Officer  
Email: DPO@northcollinscsd.org

LEA's contact for matters relating to security of Student Data:

Name: Brian Zolnowski  
Title: Data Protection Officer  
Email: DPO@northcollinscsd.org

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

**LEA: North Collins Central School District**

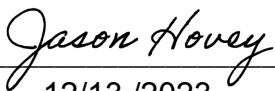
By: 

Date: 12/13/2023

Printed Name: Brian Zolnowski

Title: Data Protection Officer

**KHAN ACADEMY, INC.**

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

Date: 12/13/2023 \_\_\_\_\_

Printed Name: Jason Hovey \_\_\_\_\_

Title: Director School Partnerships \_\_\_\_\_

## 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 and state privacy laws, rules, and regulations, all as may be amended from time to time. This DPA supplements the Service Agreement and together with the Service Agreement is collectively referred to as the “**Agreement**”.
2. **Services to Be Provided.** Pursuant to and as fully described in the Service Agreement, Provider offers the digital educational services as set forth in **Exhibit “A”** hereto (the “**Services**”). Provider may update the description of the Services from time to time to reflect new products, features, or functionality comprised within the Services. Provider will update relevant documentation to reflect such changes.
3. **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”**.
4. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. With respect to the treatment of Student Data, 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, 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, or the party who provided such data (such as the student or their parent). 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, or the party who provided such data (such as the student or their parent).
2. **Exemptions under FERPA.** LEA is familiar with and agrees to be responsible for compliance with applicable laws governing the LEA’s disclosure of Personally Identifiable Information in Education Records to a third party without written consent of the parent and/or eligible student or without meeting one of the exemptions set forth in FERPA (“FERPA Exemption(s)”), including the exemption for Directory Information (“Directory Information Exemption”) or School Official exemption (“School Official Exemption”). For the purposes of FERPA, to the extent Personally Identifiable Information from Education Records are transmitted to Provider from LEA or from students using accounts at the direction of the LEA, Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, provided, that certain information provided to Provider by LEA about a student, such as student name and grade level, may be considered Directory Information under FERPA and thus not an Education Record.
3. **Parent Access.** Education Law § 2-d and FERPA provide parents the right to inspect and review their child’s or the eligible student’s Student Data stored or maintained by the LEA. The LEA shall establish reasonable procedures by which a parent 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, if supported by the functionality of Services. For the purposes of this DPA, parent refers to the parent or legal guardian of the student. Provider shall respond in a reasonably timely manner (and pursuant to the time frame required under state law for an LEA to respond to a parent or student) to the LEA's request for Personally Identifiable Information contained in a student's School Account to view or correct as necessary, consistent with the functionality of the Services. 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, provided, that parents may establish parent accounts associated with their child's account, and Provider may provide direct assistance to students and their parents relating to access to or correction of information displayed in the student's Khan Academy account, consistent with the functionality of the Services.

4. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall comply with applicable laws relating to the transfer of Student-Generated Content to a Khan Academy account held by the student or their parent. In addition, prior to deletion of Student Data at the direction of the LEA, Provider may transfer said account or Student-Generated Content to a Khan Academy account controlled by the student or their parent.
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 redirect such third party to request the data directly from the LEA, unless and to the extent that Provider reasonably believes it must grant such access to the third party because the data disclosure is necessary: (i) pursuant to a court order or legal process; (ii) to comply with statutes or regulations; (iii) to enforce the Agreement; or (iv) if Provider believes in good faith that such disclosure is necessary to protect the rights, property or personal safety of Provider's users, employees or others. Provider shall notify the LEA in advance of a compelled disclosure to a third party, unless legally prohibited.
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 and state privacy laws, rules, and regulations, all as may be amended from time to time (collectively "**Applicable Laws**"). LEA shall uphold its responsibilities under Applicable Laws, including to grant Provider access to such data only to the extent permitted by Applicable Laws. For clarity, the LEA shall not provide any data in violation of Applicable Laws and shall not provide Personally Identifiable Information beyond that which is identified in Exhibit B including, but not limited to, credit card data, personal health information, or social security numbers, unless otherwise agreed by the Parties in writing. At Provider's request, LEA will designate an employee or agent of LEA as the LEA's representative for the coordination and fulfillment of LEA's duties under this DPA.

## **2. Annual Notification of Rights.**

- a. The LEA acknowledges that under the Service Agreement, the LEA is responsible for providing appropriate disclosures to students and their parents regarding disclosure of Student Data to Provider and student use of the Services, including any notices required by the COPPA, FERPA, or other Applicable Laws, and that, prior to creation of School Accounts, the LEA will either obtain any parent consent or comply with an applicable exemption from or exception to parental consent requirements for opening School Accounts for students and use of the Service.
- b. If LEA is providing Directory Information or any Education Record to Provider, LEA shall:
  - i. comply with the Directory Information Exemption, including, without limitation, informing parents and eligible students what information the LEA deems to be Directory Information and may be disclosed and allowing parents and eligible students a reasonable amount of time to request that schools not disclose Directory Information about them; and/or
  - ii. comply with the School Official Exemption, including, without limitation, informing parents in their annual notification of FERPA rights that the Institution defines “School Official” to include service providers and defines “legitimate educational interest” to include services such as the type provided by Provider; or
  - iii. obtain all necessary parental or eligible student written consent to share the Student Data with Provider, in each case, solely to enable Provider’s operation of the Service.
- c. If LEA is relying on the Directory Information exemption, LEA shall not provide information to Provider from any student or parent/legal guardian that has opted out of the disclosure of Directory Information. Provider depends on LEA to ensure that LEA is complying with the FERPA provisions regarding the disclosure of any Student Data that will be shared with Provider.

**3. Bill of Rights for Data Privacy and Security.** As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit E and Exhibit F, respectively, and incorporated into this DPA. Pursuant to Education Law Section 2-d, the LEA is required to post the Parents Bill of Rights on its website.

**4. Reasonable Precautions.** LEA shall take reasonable physical, technical, and administrative precautions consistent with industry standards designed to secure usernames, passwords, and any other means of gaining access to the Services and hosted Student Data.

**5. Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized use of (or access to) the Services. 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.** Provider shall comply in all material respects with all applicable U.S. federal and state 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 Service to LEA.

2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than to provide the Services, for purposes authorized by the Services Agreement and/or otherwise legally permissible. The foregoing limitation does not apply to De-Identified Data.
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 shall not make any re-disclosure of any Student Data in a manner that directly identifies an individual student to any other entity other than LEA, except: (i) as directed or permitted by the LEA or this DPA, including as authorized under statutes referred to herein; (ii) to authorized users of the Services, including students and their parents; (iii) as directed or permitted by the user in accordance with the intended functionality of the Services; (iv) as permitted by law; or (v) to protect the safety or integrity of users or others, or the security of the Services. This prohibition against disclosure shall not apply to De-Identified Data, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors or agents performing services on behalf of or in conjunction with the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
5. **De-Identified Data:** De-Identified Data may be used by the Provider for any lawful purpose including, but not limited to, development, adaptive learning and customized student learning, research, and improvement of educational sites, services, and applications, and to demonstrate market effectiveness of the Services. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Provider agrees not to attempt to re-identify De-Identified Data retained after termination of the relevant user account.
6. **Disposition of Data.**
  - a. Upon written request from the LEA, Provider shall dispose of Student Data obtained under the Service Agreement. Provider shall respond to such a request for disposition in a reasonably timely manner (and pursuant to any time frame required under state law). Upon termination of the Service Agreement, if no written request from the LEA is received, individual user accounts will remain open and available for use for other educational purposes. 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."
  - b. In addition to complying with disposition requests made by the LEA, Provider may dispose of Student Data: (i) when the Student Data is no longer needed for the purpose for which it was received; (ii) in accordance with its disposition policy; or (iii) as required by law.
  - c. The duty to dispose of Student Data shall not extend to Student Data that has been De-Identified or placed in an account controlled by a student or their parent pursuant to Section II 3.
  - d. Prior to disposition of Student Data at the direction of the LEA under this section or Article II, Section 3 (Separate Accounts), Provider may permit users or parents to maintain the Khan

Academy Website account as a personal account for purposes of retaining any content generated or provided by the user (including Learning activity). Certain account controls, including the ability to modify the account profile or delete the account, may be exercisable by the teacher that created the account, by the student account holder or their parent. Requirements relating to transfer of data will be satisfied by the ability to maintain a personal account or establish a personal login credential to allow the student to maintain their account. Account transfer may not be available for some types of accounts due to limitations inherent in the functionality of the Services.

7. **Advertising Limitations.** Unless authorized by LEA or parent, Provider is prohibited from using, disclosing, or selling Personally Identifiable Information contained in Student Data to: (a) serve Targeted Advertising to students; or (b) develop a profile of a student 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); (ii) to make product recommendations to teachers or LEA employees; (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; or (iv) to communicate with users generally via the Services or by sending Program Communications to users. This provision does not restrict Provider's activities relating to personal accounts established or maintained by parents, students or teachers.

## **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. **Data Security.** The Provider agrees to utilize commercially reasonable 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 applicable to the provision of the Services. The Provider's Data Security and Privacy Plan is attached to this DPA at Exhibit "G".
3. **Data Breach.** In the event that Provider becomes aware of an unauthorized release, disclosure or acquisition of Student Data resulting in an unauthorized access to or disclosure of the Student Data maintained by the Provider in violation of applicable state or federal law or this DPA ("**Incident**"), the Provider will provide notification in seven (7) calendar days. Upon notification by the Provider, the LEA shall be responsible for reporting the Incident to its Chief Privacy Officer and/or other officials as required by law.
  - a. The security incident notification described above shall include, at a minimum, the following information to the extent known by the Provider:
    - i. The name and contact information of the reporting LEA subject to this section.
    - ii. A list of the types of Personally Identifiable Information that were or are reasonably believed to have been the subject of a breach.
    - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range



within which the breach occurred. The notification shall also include the date of the notice.

- iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
  - v. A general description of the breach Incident, if that information is possible to determine at the time the notice is provided.
- b. Provider agrees to adhere to all applicable 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.
  - c. 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. To the extent LEA determines that the security incident triggers notice requirements under Applicable Laws, LEA shall provide notice and facts surrounding the breach to the affected students and parents.
  - d. In the event of an Incident originating from LEA's use of the Service, LEA shall cooperate with Provider to the extent necessary to expeditiously secure Student Data and/or the Services.
  - e. This provision shall not restrict Provider's ability to provide separate breach notification to its customers, including parents and other individuals with personal accounts.

## **ARTICLE VI: MISCELLANEOUS**

1. **Term and Termination.** This DPA shall remain in effect for school year 2023 and 2024, expiring on June 30, 2024. This DPA will terminate simultaneously and automatically with the termination or expiration of the Service Agreement. In the event that either party seeks to terminate this DPA, they may do so by terminating the Service Agreement as set forth therein. Either party may terminate this DPA and any Service Agreement in the event of a material breach of this DPA by the other party.
2. **Termination; Survival.**
  - a. Individual user accounts created pursuant to the Services will remain open and available for use until deleted by the School using account management functions available for the Services, or by submitting a deletion request to Provider. For accounts that remain open Provider will retain basic account data (for example, username, password, date of birth) needed to maintain the account, and the user's learning activity.
  - b. At the LEA's request, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, Section 6. Prior to destruction, the Provider may transfer the account ownership to an account on the Services controlled by the student or their parent, if permitted by the functionality of the Services. Requirements relating to transfer of data will be satisfied by the ability to maintain a

personal account or establish a personal login credential to allow the student to maintain their account.

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. Except for the changes made by this DPA, the Service Agreement remains unchanged and in full force. For clarity, the liability of each party under this DPA shall be subject to the exclusions and limitations of liability set out in the Service Agreement. With respect to the treatment of Student Data, 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 cases where the LEA is making the Services available for use by teachers and students through a third party service that includes an alternative data privacy agreement to which Provider is a party, such alternative agreement shall apply, rather than this DPA.
4. **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. For clarity, nothing in this Section 5 (Entire Agreement) prohibits Provider from amending the Service Agreement pursuant to the amendment provisions set forth therein, or from amending the documentation, including Exhibits A-C, to reflect changes to the Services in the Service Agreement.
5. **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.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA SIGNING THIS DPA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES.
7. **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 the Provider sells, divests, or transfers all or a portion of its business assets to a third party, the Provider may transfer Student Data to the new owner provided that: (i) the new corporate owner intends to maintain and provide the Services as a going concern and the new owner has agreed to data privacy standards no less stringent than those provided herein; or (ii) the Provider will give notice to LEA and an opportunity to opt out of the transfer of Student

Data.

8. **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.
9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

## EXHIBIT "A"

### DESCRIPTION OF SERVICES

Khan Academy provides access to a website located at <http://khanacademy.org> and related mobile application (collectively "**Website**"), through which it provides free educational services, including, but not limited to, educational content, and to other products and services that Khan Academy may provide now or in the future (collectively, the "**Service**"). The Service is governed by and further described in Khan Academy's [Terms of Service](#) and [Privacy Policy](#).

The Website offers instructional content (principally videos and articles), practice exercises, and a personalized learning dashboard that empowers learners to study at their own pace in and outside of the classroom. Website services include a wide range of content and learning activities, including instructional content and exercises aligned to core curriculum, teacher support materials, test practice courses (for example, SAT practice) and other learning activities and education programs.

Standard 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 share their account data with other authorized users, including a parent or legal guardian ("**parent**"), or others as permitted by the intended functionality of the Services
- permit users to post or respond to questions relating to learning activities on the Website
- offer additional educational programs (Learnstorm, test prep, scholarship programs) through the Website
- in-app or emailed communications to notify users about assignments, suggest additional learning activities, activity reports, service updates (e.g., new features or content), or educational programs
- provide links to additional educational resources

Khan Academy services include research and analysis to inform the use of, and to improve and develop, the Website and educational services. Khan Academy may share De-Identified Student Data for research purposes or to demonstrate the impact of the Services.

Students or teachers may have personal accounts in addition to school accounts created by or at the direction of the school, and parents may elect to create an account on the Website associated with their child's account and monitor their learning progress via the learning dashboard. Personal account activity is governed by Provider's Website Terms of Service and Privacy Policy. This DPA does not apply to personal accounts or use of accounts via a personal login.

This DPA applies only to use of the Services through School Accounts created by or at the direction of the LEA. School Accounts are defined in, and must be established in accordance with, the [Terms of Service](#). In addition to the free Website and Services for School Accounts covered by this DPA, Khan Academy offers supplemental services to school districts and educational agencies to facilitate implementation by the district or agency, including MAP Accelerator (offered by NWEA as a complement to the MAP Growth assessment). 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 Districts, Khanmigo for Districts, and 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.	X
	Other application technology metadata-Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	X
	Place of Birth	
	Gender	O
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
	Gender is an optional field and not required to provide the Service.	
Enrollment	Student school enrollment	O
	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.	O
	Address	
	Email	

Parent/Guardian Contact Information	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	X
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 - <i>School email only</i>	O
	Phone	
Student Identifiers	Local (School district) ID number	O
	State ID number	
	Provider/App assigned student ID number	
	Student app username	X
	Student app passwords	
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	O
Student work	Student generated content; writing, pictures, etc.	
	Other student work data -Please specify:	X
	Information about use of the Website and activities on the Website.	
Transcript	Student course grades	
	Student course data	

	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	<p>Please list each additional data element used, stored, or collected by your application:</p> <p>The data provided by the LEA varies depending on LEA's practices and use of the Website, including use of rostering or single sign on services. Certain data elements identified above are provided by the account holder (user) based on the individual user's interactions with the Website.</p> <p>Items marked with a “X” are either required for provision of the Service or are customarily provided in the course of providing the Service. The data provided by the LEA typically includes data to identify the user account (username and school email address), the user's date of birth and class assignment data (teacher and assignments on the Service).</p> <p>Items marked with an “O” are optional. The LEA may provide supplemental data (for example, demographic information) or other types of data for purposes of conducting efficacy analyses, pedagogical research or similar analyses. Teachers may identify the school or school district, and may provide school district ID, including a Clever ID, when using rostering services. Grade level information may be provided or inferred from subjects studied. Collection of student email depends on the rostering method.</p> <p>Individual users may provide additional data as part of their interaction with the Services. For example, user communications may include customer support requests or optional comments posted on the Website, if provided by a user. Users may complete optional surveys and survey questions may be used in connection with optional programs offered on the Website (Learnstorm).</p> <p>LEA acknowledges that for the provision of the Services, Provider does not need (and LEA shall not send to Provider) sensitive information including social security number, driver’s license number, identification card number, tribal identification number, financial account information (PCI or otherwise), or medical or health insurance information.</p> <p>Khan Academy does not obtain Teacher or principal data, as defined in New York Education Law § 2-d, in the course of providing its Service. Khan Academy does not authorize use of the Service in performance reviews of classroom teachers or principals.</p>	O

None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	N/A
------	---	-----



## EXHIBIT "C"

### DEFINITIONS

**De-Identified Data and De-Identification:** Records and information are 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.

**Directory Information:** Directory Information shall have the meaning set forth under FERPA cited as 20 U.S.C. § 1232 g(a)(5)(A).

**Educational Records:** Education Records shall have the meaning set forth under FERPA cited as 20 U.S.C. § 1232 g(a)(4).

**Learning activity:** means information relating to an identified student's use of the Services generated by the user through the use of the Services. Learning activity that is De-Identified is not Student Data or Personally Identifiable Information.

**Personally Identifiable Information:** Personally Identifiable Information includes, without limitation, those items set forth in the definition of Personally Identifiable Information under FERPA and State regulations as identified in this DPA, if any.

**Program communications:** means in-app or emailed communications relating to Provider's educational services, including prompts, messages and content relating to use of the Services, for example: onboarding and orientation communications, prompts for students to complete, or teachers to assign exercises or provide feedback as part of a learning exercise, periodic activity reports, suggestions for additional learning activities on the Services, service updates (for example, new features or content), and information about special or additional programs that may be offered through the Service.

**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 (if supported by the Services), the student's learning activity generated through use of the Services and account information that enables ongoing ownership of such content.

**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.

**Sell:** For the purposes of this DPA, Sell shall have the meaning assigned by applicable U.S. federal or state law and shall be interpreted consistent with the Future of Privacy Forum's Student Privacy Pledge. Sell does not include sharing, transferring or disclosing Student Data with a Subprocessor that is necessary to perform a business purpose (such as detecting security incidents, debugging and repairing, analytics, storage or other processing activities) provided that the Subprocessor does not Sell the Student Data, or any sharing, transfer or disclosure of

Student Data made by the user through the functionality of the Services. Sell also does not include or apply to a purchase, merger or other type of acquisition of a company by another entity, provided that the company or successor entity continues to treat the Personally Identifiable Information contained in Student Data in a manner consistent with this DPA with respect to the previously acquired Personally Identifiable Information contained in Student Data.

**Service Agreement:** Refers to the Provider’s Terms of Service and Privacy Policy and, to the extent applicable, any additional services agreement executed between Provider and the LEA, including an executed order form or purchase order.

**Student Data:** Student Data refers to any Personally Identifiable Information, whether gathered by Provider or provided by LEA or its users pursuant to 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 or any other information that would permit identification of a specific student. Student Data includes the Learning activity of an identified student. 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 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 anonymised or aggregated, or anonymous usage data regarding usage of Provider’s Services.

**Subprocessor:** For the purposes of this DPA, the term “Subprocessor” (sometimes referred to as a “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.

**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 or mobile application based on the content displayed or in response to a student's response or request for information or feedback.

**Website:** means the Khan Academy website and related mobile applications and online services.

**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.

Provider's ability to partially dispose of data may be limited by processing system limitations; in that case, the parties will agree on the scope of disposition, or LEA may opt to specify complete disposition.

2. Nature of Disposition

\_\_\_\_\_ Disposition shall be by destruction or deletion of data.

\_\_\_\_\_ Disposition shall be by a transfer of data to individual user accounts as specified in the Service Agreement, if transfer is supported by the existing functionality of the Service.

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"**

**PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

Pursuant to Section 2-d of the New York State Education Law ("**Education Law § 2-d**"), parents and eligible students are entitled to certain protections regarding confidential student information. **Set forth below is the Parents Bill of Rights and supplemental information regarding Khan Academy Services.** Any terms not defined herein, shall have the meaning set forth in Education Law § 2-d.

1. A student's personally identifiable information cannot be Sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record maintained by the LEA.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all Student Data elements collected by the State is available for public review at <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx> or by writing to the NYS Education Department, Information & Reporting Services, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints may be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website at [www.nysed.gov/student-data-privacy/form/report-improper-disclosure](http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure).
6. Supplemental information regarding Khan Academy's services and protections for confidential student information are set forth in Exhibit F.
7. The LEA may elect to specify the name and contact information for its representative that will respond to parent inquiries and complaints below:

Name : \_\_\_\_\_  
Title: \_\_\_\_\_  
Address: \_\_\_\_\_  
Email address: \_\_\_\_\_  
Phone number: \_\_\_\_\_

## EXHIBIT "F"

### SUPPLEMENTAL INFORMATION

This document provides information for parents regarding use of the Khan Academy Service in schools in New York State. Khan Academy's services are provided under its [Terms of Service](#) (the "**Service Agreement**") posted on the Khan Academy website. This information is the "Supplemental Information" required to be provided to parents in accordance with the requirements of New York State Education Law §2-d ("**Education Law §2-d**").

- A. **Name of Provider:** Khan Academy
- B. **Service:** Khan Academy, Inc., is a nonprofit organization with a mission to provide a free, world-class education for anyone, anywhere. Through our free website located at <http://khanacademy.org> (the "**Website**"), mobile application and related services (collectively, the "**Service**"), we provide educational content and services to individual students, parents, teachers and schools.

Khan Academy provides features and tools that allow teachers or school personnel to work with Students in order to provide them with tutorial, educational and other education-related services. Each student, and each teacher, leader, aide, or other similar personnel ("**School Personnel**") enrolled in the Service is registered with an individual account on the Website. Accounts may be used for work in the classroom or for at-home learning. Parents may establish parent accounts to view their child's progress and assist them with at-home learning.

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. The Khan Academy [Privacy Policy](#) is available on the Website.

- C. **Use of Student Data:** In order to provide its Service, Khan Academy may obtain personal data, including student name, email address and date of birth, as described in its Privacy Policy. Student Data and/or Teacher or Principal Data which Provider comes into possession as part of its Agreement with the LEA shall be used for the following exclusive purpose(s):

Pursuant to and as described in the [Service Agreement](#), Khan Academy will use Student data in order to provide access to and use of Khan Academy's Services as set forth the LEA's agreement with Khan Academy (the "**Agreement**"), including (i) to provide students with individual Website accounts; (ii) to provide adaptive and/or customized student learning features of the Service and educational programs offered through the Service; (iii) to allow School Personnel, and parents and coaches associated with students, to review and evaluate student educational achievement and progress on the Service; and (iv) to communicate with users regarding use of the Service and provide information regarding educational and enrichment programs. Certain programs may be offered only with the approval of the LEA or the Parent, in accordance with applicable laws.

Khan Academy will not sell or disclose Student data to any third party for any Commercial or Marketing Purpose.

Khan Academy will implement administrative and technical safeguards designed to protect the security, confidentiality and integrity of personally identifiable Student Data in its custody.

D. **Service Providers:** In order to provide the Service, Khan Academy may share Student data with its employees, contractors and Third party service providers (such as providers of data hosting, analytics, customer support and communications services) and program partners that have a legitimate need to access such information in order to provide their services to Khan Academy. Khan Academy requires its employees, contractors and Third party service providers to agree to protect Student data and/or Principal or Teacher Data (if applicable) in a manner no less stringent than the terms of the DPA. A list of Provider's Subprocessors (which may be updated from time to time) may be accessed from the Provider's Website.

E. **Transfer or Deletion Data:**

- a. **Term:** The Agreement will remain in effect unless and until the Service Agreement is terminated by either party, as set forth in the Service Agreement.
- b. **Transfer or Disposal of Data:** Individual user accounts will remain in effect unless and until the School District or School Personnel instructs Khan Academy to delete the accounts, or the Parent or Student takes action to delete the account. Prior to terminating School Accounts at the direction of the School District or its personnel, Khan Academy may (but is not required to) invite Students or Parents to establish a personal account for purposes of retaining any content generated or provided by the Student (including the Student's learning activity). Any such personal accounts will be established under Khan Academy's standard account opening process, including by obtaining Parent consent where required by applicable law. Upon deletion of an Account, Student data received by Khan Academy will be either: (a) retained in a personal account; (b) de-identified; or (c) deleted from Khan Academy's computer systems.

F. **Parent Access and Challenges to Accuracy of Student Data:** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information contained in the related student's Education Records and correct erroneous information. Student data held by Khan Academy is accessible in the Student's account profile, and may be viewed by the Student or Parent at any time in the Student's account. Parents may elect to open a free Parent account associated with their Student's account on the Website, and will be able to view and correct the Student's account profile information and view their account activity through the Parent account. Data that is accessible in the account is limited to basic account data (such as username, password, birthdate) and information regarding Khan Academy usage data (such as videos watched and exercises completed); it does not include school data such as test scores, grades or attendance records.

If Khan Academy receives a request from a Parent requesting correction of Student data collected by Khan Academy or its subcontractors, Khan Academy will either (i) directly assist the Parent or guardian with respect to their request to correct Student data held by Khan Academy, (ii) direct their request to the Student's teacher or School for resolution by the School or (iii) request that the Parent direct their request to the Student's teacher or School for resolution by the School.

G. **Data Storage and Security Measures:** Khan Academy and the LEA hereby agree that the Student Data shall be stored in the following manner. Khan Academy shall employ administrative and technical safeguards to protect Personally identifiable information that it obtains in the course of providing its Service for School use. Khan Academy's safeguards to protect Student data include use of encryption technologies to protect data both in transit and at rest:

*Encryption of data in transit.* Khan Academy employs industry standard encryption technology to protect information and data transmitted over the internet or other public network

*Data storage and server hosting.* The Khan Academy Website is hosted on Google AppEngine as a part of Google Cloud Platform (GCP), and we rely on them for server and datacenter security. All data on GCP is encrypted at rest in accordance with Google's security practices.

Supplemental information about [Khan Academy's security practices](#) is available on the Website.

**EXHIBIT "G"**  
**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. The Khan Academy Privacy Policy (available on the Khan Academy website), informs users of Khan Academy's policies and procedures regarding the collection, use, and disclosure of their personally identifiable information. [Schools and Student Use of the Privacy Policy](#) details privacy commitments specific to school users and student records.

**Use of Student Data**

Student data will be used exclusively for providing the Service and related purposes described in the Agreement, including fulfilling School District data requests or as otherwise directed or approved by the School District.

Khan Academy does not obtain Teacher or principal data, as defined in New York Education Law § 2-d, in the course of providing its Service. Khan Academy does not authorize use of the Service in performance reviews of classroom teachers or principals.

**Data Security**

Khan Academy employs administrative, operational, and technical safeguards to protect Personally identifiable information that it obtains in the course of providing its Service for School use. These safeguards include:

*Encryption.*

In transit: Khan Academy supports and encourages the use of the latest encryption protocols for all information and data transmitted over the internet or other public networks, including TLS 1.2, AES256 encryption, and SHA256 signatures.

At rest: the Khan Academy website and mobile application are hosted in the US on Google AppEngine as a part of Google Cloud Platform (GCP), and we rely on them for server and data center security. and stability. 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. Asset owners are responsible for granting access based on the users' role. Access to Khan Academy data is granted on an individual basis as determined



by business need. All employees are required to use multi-factor authentication and strong passwords following NIST guidelines to access Khan Academy resources.

*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.

*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. Company-issued laptops are equipped with on-device threat detection and reporting capabilities.

*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; Personnel Practices**

Our employees are required to complete privacy and information security awareness training upon hire and periodically thereafter. Employees are required to acknowledge and agree to our written information security policy which, among other things, highlights our commitment to keep Student data and confidential information secure.

All Khan Academy employees are screened with background checks prior to their employment with us (subject to applicable law).

### **Third Party Service Providers**

In order to provide the Service to you, Khan Academy engages third party service providers to provide certain services such as server and data hosting, email delivery, customer service, analytics, and internal productivity and communication tools. 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 personal and confidential information shared in the context of the services relationship.

### **Incident management**

Incident response policies and procedures are in place to guide personnel in reporting and responding to data security incidents. Procedures exist to identify, report, and act upon data security incidents (or when investigating possible incidents). Our incident response plan is exercised at least annually.

Khan Academy's incident response procedures include procedures to provide prompt notification regarding security incidents as required by applicable laws, including a description of the security incident based on available information, and contact information for the Khan Academy representative(s) who will be available to assist the subscribing school district. To the extent that the incident triggers third party notice requirements under applicable laws, Khan Academy will either provide direct notification to affected persons or assist the School District in providing such notifications to affected School users. Khan Academy may concurrently provide breach notifications to its customers, including parents and other individuals with website accounts.

## **Parent Rights**

Supplemental information for Parents is included in Exhibit E. The supplemental information includes information regarding how a Parent may challenge the accuracy of Student data that is collected by Khan Academy.

A Parent, Student, eligible student, teacher or principal may challenge the accuracy of the student data that is collected by Khan Academy by notice to Khan Academy (choose "Report a problem" in Khan Academy's Help Center) or send an email to [privacy@khanacademy.org](mailto:privacy@khanacademy.org). Teachers or principals may also submit notices to [schoolpartnerships@khanacademy.org](mailto:schoolpartnerships@khanacademy.org).

Student Data held by Provider is accessible in the Student's account profile, and may be viewed by the Student or Parent at any time in the Student's account. Parents may elect to open a free Parent account associated with their Student's account on the Services, and will be able to view and correct the Student's account profile information and view their account activity through the Parent account.

In the event that Khan Academy refers a Parent, Student or Eligible student request to review or correct education records to the School District, the School District will follow the necessary and proper procedures under the Family Educational Rights and Privacy Act (FERPA) and New York Education Law §2-d. The School District will provide Khan Academy with the name and contact information (including email) of the School District 's representative that will be responsible for responding to any such request. Khan Academy will respond in a reasonably timely manner to the School District's request for assistance with any request to view or correct Student data held by Khan Academy, consistent with the functionality of the Services.

### **Deletion or transfer upon termination of accounts**

Services will be provided until either party terminates the Service. School Personnel may terminate the Services individually and/or with respect to School Accounts created by such School Personnel by contacting Khan Academy at [schoolpartnerships@khanacademy.org](mailto:schoolpartnerships@khanacademy.org). Khan Academy will dispose of Student accounts and Personally identifiable information contained in Student accounts within a reasonable time period following a written request from the School District, as described below, subject to Khan Academy's ability to retain data in a personal account (described in Exhibit E – Data Deletion upon Termination).

Absent an agreement between Khan Academy and the School District, Personally identifiable information will be disposed of rather than returned to the School District, except that if a Student chooses to establish or maintain a personal account with Khan Academy, Personally identifiable information required to establish the account and maintain the content will be retained. Methods of disposition include erasing any Personally identifiable information contained in Student Data or permanently encrypting or otherwise modifying the Personally identifiable information contained in Student data to make it unreadable or indecipherable, de-identified or anonymized. The duty to dispose of Student Data shall not extend to data that has been rendered unreadable or indecipherable, de-identified or anonymized.

Khan Academy may review and update this Data Security and Privacy Plan from time to time, provided that any such updates shall not materially diminish the overall security of the Service or Student Protected Data.