STUDENT DATA PRIVACY ADDENDUM

between

the LEA named herein

and

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

a vendor provided DPA

This Student Data Privacy Addendum ("**DPA**") is incorporated by reference into the Service Agreement (as defined in **Exhibit "C" [the "Definitions"]**) entered into by and between the customer 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 last date of signature ("**Effective Date**").

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

WHEREAS, the 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; 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. 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 Kids application and related services:

Allison Leedie, Partnerships Team
Khan Academy, Inc. Attn: Khan Kids
P.O. Box 1630, Mountain View, CA 94042
khankidspartners@khanacademy.org

All legal notices shall also be sent by email to notices@khanacademy.org.

The designated representative for the LEA for this DPA is:

Name: Chrysti Silva
Title: Tech Support Field Coordinator
Address: 1340 State St. Salem OR. 97301
Email: silva_chrysti@salkeiz.k12.or.us

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

LEA:

By: _Chrysti Silva_____

Date: 11/22/2024_____

Printed Name: _Chrysti Silva_____

Title: _Tech Support Field Coordinator_____

KHAN ACADEMY, INC.

By: _____

Date: _____12/2/24_____

Printed Name: _Caroline Hu Flexer_____

Title: _VP, Khan Academy Kids_____

Type text here

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 Services as set forth in **Exhibit "A"** hereto. 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**. To the extent required by law, 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

4

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 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.

5. **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.

6. **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, including any laws referred to in the Exhibits hereto (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 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. **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.

4. **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**. The 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. For clarity, the parties may identify the specific applicable , state laws, rules, and regulations in this DPA, including the Exhibits hereto.

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 permitted by law; or (iv) 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 performing services on behalf of 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

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 parent pursuant to Article II, Section 3 (**Parent Access**).

   d. Prior to disposition of Student Data at the direction of the LEA under this section or Article II, Section 4 (**Separate Accounts**), Provider may permit users or parents to maintain the Services as a personal account for purposes of retaining any content generated or provided by the user (including Learning activity).   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.

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 the most expedient time possible and without unreasonable delay (and within any notice period required by law). 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 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 an Incident;
   iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the Incident, (2) the estimated date of the Incident, or (3) the date range within which the Incident occurred and 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 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 an Incident related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Incident.

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 an Incident triggers notice requirements under Applicable Laws, LEA shall provide notice and facts surrounding the Incident 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 2024 and 2025, expiring on June 30, 2025. 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 App, or by submitting a deletion request to Provider. For accounts that remain open Provider will retain basic account data (for example, username, password, age) needed to maintain the account, and the user's 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.

b. At the LEA's request, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, Section 6 (**Disposition of Data**). 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.

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 4 (**Entire Agreement**) prohibits Provider from amending the Service Agreement pursuant to the amendment provisions set forth therein, or from amending 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

KKIDSGR1.2024

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 Kids is a mobile application owned and operated by Khan Academy (the "**App**"). The App is provided for free. This DPA applies to use of the App by preschool providers, Head Start classroom programs, schools and school districts (collectively, the "**Schools**") as part of the School's educational curriculum (the "**Services**"). The Service is governed by and further described in Khan Academy's Terms of Service, the Khan Kids Privacy Policy, and, to the extent applicable, any additional district-level Services Agreement executed between LEA and Provider.

The App is an educational mobile application designed for young learners. The App provides educational content and activities in core subjects like early literacy, reading, writing, language, art, and math. The App features include:

- teacher tools to set up their class
- permit users to sign in with class codes
- ability to assign lessons to students and monitor student progress

Khan Academy may enter into supplemental services agreements with the LEA to provide additional support for institutional implementation, including rostering support, professional development, administrator access, and usage reports.

The App is downloaded to a personal device such as a tablet. Parents may view their child's information (user name and learning activities completed) at any time in the App by logging in to the child's class account using the child's class code (if one is provided) or by viewing the App if it is downloaded on a personal device used in the home.

The Services include research and analysis to inform the use of and to improve and develop the Services and educational services.

The App is available for individuals, including teachers and parents, for personal use. These accounts are personal accounts governed by the Terms of Service entered into between Khan Academy and the parent, and are not School Accounts. 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.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Metadata	IP Addresses of users, Use of cookies, etc.	X
	Other application technology metadata - Please specify:	
Application Use Statistics	Metadata 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)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information - Please specify:	
Enrollment	Student school enrollment	O
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information - Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Schedule	Student scheduled courses	
	Teacher names	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 - *School email only*	
	Phone	
Student Identifiers	Local (School district) ID number	
	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	
Student work	Student generated content; writing, pictures, etc.	
	Other student work data - Please specify:	X
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	Please list each additional data element used, stored, or collected by your application:	
	The App is designed to minimize the collection and use of personally identifiable data. The data provided by the LEA varies depending on LEA's practices and use of the Service. The data provided by the LEA typically includes data to identify the user account. For accounts created by teachers, we recommend use of a nickname or other account name not containing Personally Identifiable Information. For accounts rostered via Clever SecureSync, the user name may include the first name, last initial, or first name, last name.	
	*LEA acknowledges that for the provision of the Service, 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), **personal contact information, social media handles,** or medical or health insurance information.*	
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	N/A

App: The Khan Academy Kids mobile applications and online services.

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).

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

Learning Activity: Information relating to an identified student's use of the Services. Learning Activity that is De-Identified is not Student Data or Personally Identifiable Information.

Personally Identifiable Information (or PII): 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: In-product or emailed communications relating to Provider's educational services, including prompts, messages and content relating to use of the Services. Examples include, without limitation, 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, service updates (e.g., new features or content), and information about special or additional programs that may be offered through the Service.

Student Generated Content: 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 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: 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.

16

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