STANDARD STUDENT DATA PRIVACY AGREEMENT

(NDPA Standard Version 1.0)

The School Board of Duval County, Florida

and

Khan Academy, Inc., a 501(c)(3) Organization

Provider Name

DCPS-Version: 1r10

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between:

The School Board of Duval County, Florida , located at 1701 Prudential Drive, Jacksonville, FL 32207
(the "**Local Education Agency**" or "**LEA**")

And Khan Academy, Inc. located at P.O. Box 1630, Mountain View, CA 94042 (the "**Provider**").
Provider Name Street, City, State

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

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

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

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

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

2. **Special Provisions.** ***Check Box if Required***
   ☐ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
   ☑ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H"**. (Optional)
   ☑ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

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

4. This DPA shall stay in effect for three (3) years. **Exhibit "E"** will expire three (3) years from the date the original DPA was signed.

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

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

The designated representative for the LEA for this DPA is:

Name: Dr. Dana Kriznar Title: Superintendent

Address: 1701 Prudential Drive, Jacksonville, FL 32207

Phone: 904-390-2000 Email: _____

The designated representative for the Provider for this DPA is:

Name: Jason Hovey Title: Director of School Partnerships

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

Phone: 415-309-6851 Email: districts@khanacademy.org

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

LEA, The School Board of Duval County, Florida

District By: _____

Printed Name: Dr. Dana Kriznar Date: 4/8/24

Title/Position: Superintendent of Schools

Khan Academy, Inc., a 501(c)(3) organization

Name of Provider

By: _____ Date: 4/2/2024

Printed Name: Jason Hovey Title/Position: Director School Partnerships

Form Approval and Review of Terms and Conditions and Privacy Policy

The online educational service's terms of service and privacy policy have been reviewed to ensure compliance with state and federal privacy laws, including FERPA and its implementing regulations, the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. ss. 6501-6506, and Section 1002.22, F.S.

By: _____

Office of Policy & Compliance ☑ Office of General Counsel ☐

STANDARD CLAUSES

Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
3. **DPA Definitions**. The definition of terms used in this DPA is found in **Exhibit "C"**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect

to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non- public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data**: Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.

6. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**. 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"**.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

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

2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

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

4. **Data Breach**. In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

    (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
        i. The name and contact information of the reporting LEA subject to this section.
        ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
        iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and

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

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

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

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

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination**. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

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

3. **Priority of Agreements**. This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between

Exhibit "H", the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

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.

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, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

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

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

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

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

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

Khan Academy may engage in research studies or assist the LEA in conducting research and other studies at the request or direction of the LEA. Students or teachers may have personal accounts in addition to School Accounts and may associate their School Accounts with their personal accounts. Additionally, they may choose to create personal login information to their School Account to provide access to the account for activity outside of school ("Personal Login"). Parents may elect to create a personal account on the Website associated with their child's account and monitor their child's learning activity. This DPA does not apply to personal accounts (or information users provide to Khan Academy through such personal accounts). Khan Academy may provide direct assistance to students and their parents requesting access to information in the student's Khan Academy account. Personal account activity is governed by Provider's Website Terms of Service & Privacy Policy). In addition to the District Services for School Accounts covered by this DPA, Khan Academy allows users to create free Website accounts, and offers supplemental services to school districts to facilitate implementation by the district (provided under separate terms). This DPA does not apply to Khan Academy Kids mobile application, Khan Academy Kids Classroom Service, or MAP Accelerator services.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	☑
	Other application technology meta data-Please specify:	☐
Application Use Statistics	Meta data on user interaction with application	☑
Assessment	Standardized test scores	☐
	Observation data	☐
	Other assessment data-Please specify: Khan Academy may obtain access to standardized test scores in order to create personalized learning plan.	☐ O
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	☐ O
	Ethnicity or race	☐
	Language information (native, or primary language spoken by student)	☐

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify: Gender is an Optional field and not required to provide Service.	☐ O
Enrollment	Student school enrollment	☑
	Student grade level	☑
	Homeroom	☐
	Guidance counselor	☐
	Specific curriculum programs	☐
	Year of graduation	☐
	Other enrollment information-Please specify: Teachers may choose to identify the school. Grade level information may be provided or inferred from subjects studied.	☐ O
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	☑
Special Indicator	English language learner information	☐
	Low income status	☐
	Medical alerts/ health data	☐

Category of Data	Elements	Check if Used by Your System
	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	☐ O
	Phone	☐
Student Identifiers	Local (School district) ID number	☑
	State ID number	☐
	Provider/App assigned student ID number	☑
	Student app username	☑
	Student app passwords	☐
Student Name	First and/or Last	☑
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	☐
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	☐
Student Survey Responses	Student responses to surveys or questionnaires	☐ O
Student work	Student generated content; writing, pictures, etc.	☐

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify: Info about use of the Website and activities on the Website, including and engagement w/ Khanmigo.	☑
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: Please see description in Exhibit H.	☑
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

EXHIBIT "C"

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

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

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

Student Generated Content: The term "Student-Generated Content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

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

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

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

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

The School Board of Duval County, Florida 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:

Categories of data

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

2. Nature of Disposition

Disposition shall be by destruction or deletion of data.

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

3. Schedule of Disposition

Data shall be disposed of by the following date:

As soon as commercially practicable.

By Date:

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Provider Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and The School Board of Duval County, Florida ("Originating LEA") which is dated 4/5/24 to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

privacy@khanacademy.org

Khan Academy, Inc., a 501(c)(3) Organization

Name of Provider

BY: Jason Hovey Date: 4/2/2024

Printed Name: Jason Hovey Title/Position: Director School Partnerships

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between (Originating LEA) and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: Dr. Dana Kriznar Title: Superintendent

Address: 1701 Prudential Drive, Jacksonville, Florida, 32207

Telephone Number: 904-390-2000 Email: _____

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

2/24/2020

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

Cybersecurity Frameworks

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

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

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

EXHIBIT "G"

Supplemental SDPC State Terms for Florida

Version 2

[The State Supplement is an optional set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual parties and will be posted on the SDPC website to provided the authoritative version of the terms. Any changes by the LEAs or Providers will be made in amendment form in an Exhibit (Exhibit "H" in this proposed structure).]

NONE.

EXHIBIT "H"

Additional Terms or Modifications

Version March 15, 2024

LEA and Provider agree to the following additional terms and modifications:
(This is a free text field that the parties can use to add or modify terms in or to the DPA. If there are no additional or modified terms, this field should read "None." 618-1/4715859.1)

Section 3, Page 2. The first sentence is hereby deleted and the following inserted in lieu thereof: "In the event of a conflict between the SDPA Standard Clauses and the Special Provisions, the Special Provisions will control.

Article II, Section 1. The following sentences are hereby deleted:
"All Student Data transmitted to Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of LEA."
"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 LEA."

Article II, Section 2. The following sentences are hereby added:
"Notwithstanding the foregoing, Provider may provide direct assistance to the parent relating to parent accounts, and parents may view (but not modify or delete) information in the student's account."

Article II, Section 3. The following sentences are added:

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

Article IV, Section 1. The following is added to the end of the sentence:

", applicable to Provider in providing the Services to LEA. For the purposes of this DPA, state and local laws, rules, and regulations are those identified in this DPA."

"Program Communications" means in-app or emailed communications relating to the educational Services, including prompts, messages and content relating to the use of the Services, for example; onboarding and orientation communications, recommendations for use of the Services, prompts for students to complete, or teachers to assign exercises or provide feedback as part of the learning exercise, periodic activity reports, suggestions for additional learning activities in the Services, service updates, and information about special or additional programs offered through the Services or offered to complement the programs offered through the Services."

Article IV. The following is hereby inserted as a new Section 8:

"8. Notwithstanding anything in this DPA to the contrary, if a Student elects (either on a paper or electronic assessment or through the Student's account on the Provider's website) to have their Student Data provided to third parties, including colleges or universities, Provider's provision of such Student's Student Data to third parties for the purpose of connecting Students with colleges and universities shall not constitute a breach of this Agreement. "

Article V, Section 2. The Section is hereby deleted and the following inserted in lieu thereof:

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

Article V, Section 5. The first sentence is hereby deleted and the following inserted in lieu thereof:
"In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seven (7) days of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. For clarity, this Section (Art. V, Sec. 5) shall not restrict Provider's ability to provide separate breach notification to its users with personal accounts."

Article VII, Section 1. The second sentence hereby deleted and the following inserted in lieu thereof:

"Either party may terminate this DPA and any Service Agreement if the other party breaches any terms of this DPA."

Article VII, Section 2. This Section is hereby deleted in its entirety.

"Program Communications" means in-app or emailed communications relating to the educational Services, including prompts, messages and content relating to the use of the Services, for example; onboarding and orientation communications, recommendations for use of the Services, prompts for students to complete, or teachers to assign exercises or provide feedback as part of the learning exercise, periodic activity reports, suggestions for additional learning activities in the Services, service updates, and information about special or additional programs offered through the Services or offered to complement the programs offered through the Services."

Article IV. The following is hereby inserted as a new Section 8:

"8. Notwithstanding anything in this DPA to the contrary, if a Student elects (either on a paper or electronic assessment or through the Student's account on the Provider's website) to have their Student Data provided to third parties, including colleges or universities, Provider's provision of such Student's Student Data to third parties for the purpose of connecting Students with colleges and universities shall not constitute a breach of this Agreement. "

Article V, Section 2. The Section is hereby deleted and the following inserted in lieu thereof:

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

Article V, Section 5. The first sentence is hereby deleted and the following inserted in lieu thereof:
"In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seven (7) days of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. For clarity, this Section (Art. V, Sec. 5) shall not restrict Provider's ability to provide separate breach notification to its users with personal accounts."

Article VII, Section 1. The second sentence hereby deleted and the following inserted in lieu thereof:

"Either party may terminate this DPA and any Service Agreement if the other party breaches any terms of this DPA."

Article VII, Section 2. This Section is hereby deleted in its entirety.

Exhibit B, page 19, Other, the following is inserted:

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.

Items marked with a "check" 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).

Items marked with an "O" are optional. The LEA may provide supplemental data (for example, demographic information, test scores) or other types of data for purposes of conducting efficacy analyses, pedagogical research or similar analyses. Collection of student email depends on the rostering method. If the LEA rosters through Clever or ClassLink, then the Clever ID (or ClassLink ID, as may be applicable) is sent for rostering.

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).

Khanmigo uses the ChatGPT technology provided by a subprocessor, OpenAI. This educational AI-powered learning tool offers both interactive activities and chat functionality resulting in user generated content prompted by user inputs. Learners are instructed not to include personal data in inputs.

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.

Exhibit C Definitions, is amended to read as follows with the changes shown in underlined text:

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose in connection with the Services, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Learning activity. 'Learning activity' means information relating to an identified student's use of the Website generated by the user through use of the Website. ~~Student Data includes Meta Data.~~ Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in Exhibit "B" is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not include De-Identified Data or ~~constitute that~~ information that has been anonymized ~~or de-identified~~, or anonymous usage data regarding a student's use of Provider's services.

Exhibit G. Exhibit G is hereby deleted in its entirety.