

CLASSDOJO STUDENT DATA PRIVACY ADDENDUM

This Student Data Privacy Addendum (“DPA”) is incorporated by reference into the Service Agreement (as defined below) entered into by and between the educational agency set forth below (hereinafter referred to as “LEA”) and ClassDojo (hereinafter referred to as “Provider”) effective as of the date the DPA is accepted by LEA (“Effective Date”) (each of Provider and LEA, a “Party” and together “Parties”). The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider and LEA have entered into certain contractual documents (which collectively are referred to as the “Service Agreement”), to provide certain Services to the LEA as set forth in the Service Agreement and this DPA (collectively the “Agreement”);

WHEREAS, the Provider is providing education or digital services to LEA; and

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), 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. **Standard Schedule.** A description of the Service Agreement, and the categories of Student Data that may be processed by the Provider on behalf of LEA, and other information specific to this DPA are attached as **Exhibit “A”** (“Standard Schedule”).
2. **Services.** The digital educational services and any other products and services that Provider may provide now or in the future to LEA pursuant to the Agreement (the “Services”) as set forth in the Standard Schedule.
3. **Standard Clauses.** The Student Data Protection Clauses (“Standard Clauses”)¹ attached hereto as **Exhibit “B”** are hereby incorporated by reference into this DPA in their entirety.
4. **Priority of Agreements.** With respect to the treatment of Student Data only, 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. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect, including, without limitation, any license rights, limitation of liability or indemnification provisions.
5. **Term.** This DPA shall stay in effect for three years, unless and until the extent terminated by the Parties.
6. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by written notice terminating the Service Agreement as set forth therein. Either party may terminate this DPA and the Service Agreement if the other party breaches any material terms of this DPA.
7. **Effect of Termination.** If the Service Agreement is terminated, the Provider shall dispose of or return all of LEA’s Student Data pursuant to Article IV, Section 5 of the Standard Clauses.
8. **Notices.** All notices or other communication required or permitted to be given hereunder must be made in writing and may be given via e-mail transmission, or first-class mail, sent to the designated representatives set forth in the Standard Schedule.

¹ Modeled after the Student Data Privacy Consortium’s (SDPC) National Student Data Privacy Model Clauses with changes to reflect how the Service operates.

9. **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 prohibits Provider from amending the Service Agreement pursuant to the amendment provisions set forth therein.
10. **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.
11. **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 THE DPA, 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.
12. **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 (“**Change of Control**”), the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of such Change of Control. 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.
13. **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.
14. **Electronic Signature:** The Parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with applicable state and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of their electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Signatory Information

By signing below, I accept this DPA on behalf of the LEA. I represent and warrant that (a) I have full legal authority to bind the LEA to this DPA, (b) I have read and understand this DPA, and (c) I agree to all terms and conditions of this DPA on behalf of the LEA that I represent.

Name of LEA: Helena School District 2
Address: 1325 Poplar St.
Lewis & Clark
Country: _____
LEA Authorized Representative full name: Siobhan K. Mathhorn
Title: Board Chair
Email: shathorn@helena-schools.org
LEA Authorized Representative signature: Siobhan K. Mathhorn
Date: 4/25/24

ClassDojo Representative signature: Elisette Weiss
Authorized Representative full name: Elisette Weiss
Title: District Partnerships
Email: privacy@classdojo.com
Address: 735 Tehama Street
San Francisco, CA 94103, USA
Date: July 16, 2023

EXHIBIT "A"
STANDARD SCHEDULE

1. **Service Agreement:** ClassDojo Terms of Service located at: <https://www.classdojo.com/terms/>
2. **Services:**

ClassDojo is a school communication and classroom management platform that helps bring teachers, school leaders, families, and students together. ClassDojo provides the following through its platform:

- Communication tools to help teachers, students, and parents or families connect with each other, provided however, that the parties agree that any family messaging, including parent-to-parent messaging or parent-to-parent groups where a teacher is not included ("Family Messaging") are not part of the Services
- A way for teachers to give feedback and assignments to students, and other classroom management tools
- A way for teachers to share photos, videos, files, and more from the classroom for families and students to see
- A way for families and students to post comments and "likes" on Class Story and School Story
- Student portfolios, where students can share their work with teachers and families
- Activities and other content that teachers or families can share with students
- A way for school leaders to see how connected their school community is, and also to communicate with families, other teachers, and school leaders
- "School Dojo Island" or "Class Dojo Island"- a virtual playground for students and their classmates where they'll explore a variety of activities focused on creativity and collaboration to explore, build, and live in a world with their classmates at the direction of their teacher. Note, however, that ClassDojo also has an out-of-school Dojo Island ("Home Dojo Island") that the parties agree is not part of the Services.
- ClassDojo Plus - an optional, paid subscription that provides additional ways for families to stay engaged with their school community and celebrate their child's growth. Note, however, that ClassDojo Plus has out-of-school features such as Home Points, At-Home Child Monster with premium parts, and Discover tab content that the parties agree are not part of the Services.

More information on how the Service operates is located at www.classdojo.com.

The Service shall not include any Outside School Accounts (as defined in the Model Clauses), Family Messaging, or Home Islands. Additionally, the Service shall not include any online live tutoring services offered for children through the website located at <https://tutoring.classdojo.com> ("Dojo Tutoring"). An Outside School Account is used for Family Messaging, Home Island play, and Dojo Tutor. An Outside School Account of a student may also be linked to their student account. Similarly, an Outside School Account of a parent or family may be linked to their parent or family account used in school. Student Data shall not include information a student, parent, or family provides to Provider through such Outside School Accounts independent of the student's, parent's, or family's engagement with the Services at the direction of the LEA. Additionally, any information a parent or family provides to Provider through such Outside School Account shall not be considered school data or information and shall not be owned or controlled by the LEA.

3. **Notices:** In the event a written notice is to be provided pursuant to the DPA, notice shall be provided to the following recipients:

Notices to Provider

ClassDojo, Inc
735 Tehama Street, San
Francisco, CA 94103
privacy@classdojo.com, with a copy to legalprocess@classdojo.com

Notices to LEA

LEA Name: _____
LEA Mailing Address: _____
LEA E-Mail Address: _____
With a copy to LEA Legal Counsel (if
provided). _____
LEA Legal Counsel Address: _____

4. **Student Data Security Inquiries Contact:**

Name: _____
Title: _____
E-Mail Address: _____

5. **LEA Contact for Parent Inquiries Pursuant to Section 2.2:**

Name: _____
Title: _____
E-Mail Address: _____

Provider Contact:

Elisette Weiss, District Partnerships, privacy@classdojo.com

6. **Schedule of Student Data:** The following specific items or categories of Student Data may be processed by the Provider on behalf of LEA for the purpose of the Services (collectively, the "**Schedule of Student Data**").

SCHEDULE OF STUDENT DATA**

In order to perform the Services, the Student Data or school data (e.g. parent or teacher data as specifically noted) processed by Provider on behalf of LEA is set forth below: **LEA should not provide any medical or health-related data.**

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	✓ https://www.classdojo.com/cookies-policy
	Other application technology metadata.	✓ https://www.classdojo.com/transparency
Application Use Statistics	Metadata on user interaction with application	✓ We track product events and progress within a particular feature
Assessment	Standardized test scores	N/A
	Observation data	✓ Optional, only if teacher(s) opt to use the “Feedback Points” feature is this collected from teachers about students. <i>Note this data is automatically deleted on a rolling 365-day basis.</i>
	Other assessment data	N/A
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	✓ Optional, only if teacher(s) elect to record
Communications	Online communications captured (emails, blog entries)	✓ Optional, only if students opt to message the teacher directly via Portfolios or Class Story. <i>Note, Family Messaging is not considered Student Data.</i>
Biometric Data	Physical or behavioral human characteristics that can be used to identify a person (e.g. fingerprint scan, facial recognition)	N/A from students; may use to validate parents/teachers with iOS or Android technology - we are not passed the information.
Conduct	Conduct or behavioral data	✓ Optional, only if teacher(s) opt to use the “Feedback Points” feature is this collected from teachers about students. <i>Note this data is automatically deleted on a rolling 365-day basis.</i>
Demographics	Date of Birth	✓ Note, this is collected as age, not a DOB.
	Place of Birth	N/A

	Gender	N/A, Not from students. Note, upon account creation for adults (family members or teachers) we optionally ask for a salutation that may indicate gender such as Mr., Miss, etc.
	Ethnicity or race	N/A
	Language information (native, or primary language spoken by student)	✓ Obtained via browser/device preferences
	Other demographic information- Please specify:	N/A
Enrollment	Student school enrollment	✓
	Student grade level	✓
	Homeroom	N/A
	Guidance counselor	N/A
	Specific curriculum programs	N/A
	Year of graduation	N/A
	Other enrollment information- Please specify:	N/A
Parent/Guardian Contact Information	Address	N/A
	Email	✓ Optional, only if a parent or guardian account is created and connected to a student
	Phone	✓ Optional, only if a teacher invites a parent or guardian to connect via SMS
Parent/Guardian ID	Parent ID number (created to link parents to students)	✓
Parent/Guardian Name	First and/or Last	✓ Optional, only if a parent account is created at the invitation of the teacher(s) or school leader(s).
Schedule	Student scheduled courses	N/A
	Teacher names	✓ This is only for the classes a student is connected to, it may not be the complete schedule of all teachers the student has classes with.
Special Indicator	English language learner information	N/A

	Low-income status	N/A
	Medical alerts/ health data	N/A
	Student disability information	N/A
	Specialized education services (IEP or 504)	N/A
	Living situations (homeless/foster care)	N/A
	Other indicator information-Please specify:	N/A
Student Contact Information	Address	N/A
	Email	✓ Only for students whose teachers elect to utilize the Google Login method.
	Phone	N/A
Student Identifiers	Local (School district) ID number	✓
	State ID number	N/A
	Provider/App assigned student ID number	✓
	Student app username	✓
	Student app passwords	✓
Student Name	First and/or Last	✓ Only as provided by the teacher(s) or school leader(s). Initials or unique identifiers may be used.
Student In-App Performance	Program/application performance (typing program- student types 60 wpm, reading program-student reads below grade level)	✓ We track product events and progress within a particular feature
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	N/A
Student Survey Responses	Student responses to surveys or questionnaires	N/A
Student work	Student-generated content; writing, pictures, etc.	✓ Note these may also be teacher-assigned projects.

	Other student work data -Please specify:	N/A
Transcript	Student course grades	N/A
	Student course data	N/A
	Student course grades/ performance scores	N/A
	Other transcript data - Please specify:	N/A
Transportation	Student bus assignment	N/A
	Student pick up and/or drop off location	N/A
	Student bus card ID number	N/A
	Other transportation data – Please specify:	N/A
Other	Please list each additional data element used, stored, or collected by your application:	**
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	N/A

**** Please see the Information Transparency Chart (<https://www.classdojo.com/transparency>) for additional details regarding:**

- Categories of Student Data
- Categories of Data Subjects the Student Data is collected from and the source of the Student Data
- Nature and purpose of the Processing activities of the Student Data
- Country in which the Student Data is stored
- List of any Special Categories of Student Data collected (currently none)
- Categories of other non-student school users (e.g. teachers, school administrators, and parents) data collected

Current list of Sub-Processors: <https://www.classdojo.com/third-party-service-providers/>

EXHIBIT "B"
STANDARD CLAUSES

July 2023

PURPOSE AND SCOPE

- 1.1. **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.
- 1.2. **Exemptions under FERPA.** LEA may not generally disclose Personally Identifiable Information from an eligible student's Education Record 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, 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 control and direction of the LEAs, with respect to Education Records and Student Data. Additionally, 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 subject to the restrictions for Education Records.
- 1.3. **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, Terms of Service, Privacy Policies etc.

2. DATA OWNERSHIP AND AUTHORIZED ACCESS

- 2.1. **Student Data Property of LEA.** As between LEA and Provider, all Student Data processed by the Provider pursuant to the 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 also 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 parent).
- 2.2. **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 the Services. If LEA is not able to update the Student Data itself, 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 an Education Record 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, provided however, that Provider may also allow for direct access requests (but not correction or deletion rights) of Student Data and/or Education Records from a verified parent.
- 2.3. **Separate Account.** Students, parent, and family users may have personal or non-school accounts (i.e. for use of ClassDojo at home not related to school) in addition to school accounts ("**Outside School Account(s)**"). An Outside School Account of a student may also be linked to their student account. Similarly, an Outside School Account of a parent or family may be linked to their parent or family account used in school. Student Data shall not include information a student, parent or family provides to Provider through such Outside School Accounts

independent of the student's or parent's engagement with the Services at the direction of the LEA. Additionally, any information a parent or family provides to Provider through such Outside School Account shall not be considered school data or information and shall not be owned or controlled by the LEA. Additionally, If Student Generated Content is stored or maintained by the Provider as part of the Services, Provider may, at the request of the LEA, or the student or the student's parent or legal guardian, transfer said Student Generated Content to a separate student account or the Outside School Account upon termination of the Service Agreement; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service.

- 2.4. Third Party Requests.** Should a third party, excluding a Sub-Processor, including, but not limited to, 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 the Requesting Party to request the Student Data directly from the LEA and shall not provide the requested Student Data to the Requesting Party, unless and to the extent that Provider reasonably believes it is compelled to 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 the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request or otherwise legally prohibited.
- 2.5. Sub-Processors.** Provider shall enter into written agreements with all Sub-Processors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Agreement, whereby the Sub-Processors agree to protect Student Data in a manner no less stringent than the terms of this DPA. The list of Provider's current Sub-Processors can be accessed through the Provider's Privacy Policy (which may be updated from time to time).

3. DUTIES OF LEA

- 3.1. Provide Data in Compliance with Applicable Laws.** LEA shall use the Services 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.
- 3.2. 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 FERPA rights (“**Annual Notification of Rights**”). Additionally, LEA represents, warrants and covenants to Provider, as applicable, that LEA has:
- a. Complied with the School Official Exemption, including, without limitation, informing parents in their Annual Notification of Rights that the LEA defines “school official” to include Sub-Processors such as Provider and defines “legitimate educational interest” to include services such as the type provided by Provider; and/or
 - b. Complied 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
 - c. Obtained 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.

If LEA is relying on the Directory Information exemption, LEA represents, warrants, and covenants to Provider that it 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.

- 3.3. **Reasonable Precautions.** LEA shall employ administrative, physical and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted data from unauthorized access, disclosure or acquisition by an unauthorized person.
- 3.4. **Unauthorized Access Notification.** LEA shall notify Provider promptly, but in no event less than 72 hours, of any known or suspected unauthorized use or access of the Services, LEA's account or Student Data. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized use or access.z

4. DUTIES OF PROVIDER

- 4.1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security applicable to the Provider in providing the Service to the LEA, all as may be amended from time to time.
- 4.2. **Authorized Use.** The Student Data shared pursuant to the 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 law.
- 4.3. **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.
- 4.4. **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 Agreement. This prohibition against disclosure shall not apply to (i) De-Identified information, (ii) Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, (iii) to Sub-Processors performing services on behalf of the Provider pursuant to this DPA, (iv) to authorizes users of the Services, including parents or legal guardians, or (v) to protect the safety or integrity of users or others, or the security of the Services. Provider will not Sell Student Data to any third party.
- 4.5. **De-Identified Data.** Provider agrees not to attempt to re-identify De-Identified Student Data without the written direction of LEA. De-Identified Student Data may be used by the Provider for those purposes allowed under FERPA and applicable state student privacy laws, as well as the following purposes (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) research development and improvement 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. Provider agrees not to transfer De-Identified Student Data to any third party unless that party agrees in writing not to attempt re-identification. Prior to publicly publishing any document that names the LEA, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Student Data is presented.
- 4.6. **Disposition of Data.** Upon written direction or initiation from the LEA, Provider shall dispose of, delete, 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 or 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 or delete all Student Data at the earliest of (a) Provider's standard destruction schedule, if applicable; (b) when the Student Data is no longer needed for the purpose for which it was received; or (c) as otherwise required by law. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to Section 2.3. 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”**.

- 4.7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or Selling Student Data (a) to inform, influence, or enable Targeted Advertising; (b) to develop a profile of a student, for any purpose other than providing the Service to LEA, or as authorized by the parent or legal guardian; or (c) for any commercial purpose other than to provide the Service to LEA, as authorized by the LEA or the parent/guardian, or as permitted by applicable law. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations or sending Program Communications to account holders); or (ii) to make product recommendations to teachers, LEA employees, or parents/legal guardians; 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.

5. DATA SECURITY AND BREACH PROVISIONS

- 5.1. **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.\
- 5.2. **Audits.** No more than once per contract year, or following a Security Incident, 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, during normal business hours and at a time convenient for the Provider, 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 (“**Security Audit**”). In connection with any Security Audit, 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, as reasonably necessary to fulfill the requests of such Security Audit. Costs for the Security Audit are the responsibility of the LEA. Provider may provide an independent third-party report in place of allowing LEA to conduct such Security Audit.
- 5.3. **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 “E”**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “E”**. 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.
- 5.4. **Data Breach.** In the event that Provider confirms an unauthorized release, disclosure of, or access to Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider in violation of applicable federal or state law (a “**Security Incident**”), the Provider shall provide notification to LEA as required by the applicable state law, but in no event later than seventy-two (72) hours of confirmation of the Security Incident (“**Security Incident Notification**”), unless notification within this time limit would disrupt investigation of the incident, by either the Provider or by law enforcement. In such an event, the Security Incident Notification shall be made within a reasonable time after the discovery of the Security Incident. A Security Incident does not include the good faith acquisition of Student Data by an employee or agent of Provider for a legitimate purpose, provided that the Student Data is not used for a purpose unrelated to the Provider’s Service or subject to further unauthorized disclosure. Provider shall follow the following process:
- 5.4.1 Unless otherwise required by applicable state law, the Security Incident Notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

1. The name and contact information of the reporting Provider subject to this section.
2. A list of the types of PII that were or are reasonably believed to have been the subject of the Security Incident.
3. If the information is possible to determine at the time the notice is provided, then either (a) the date of the Security Incident, (b) the estimated date of the Security Incident, or (c) the date range within which the Security Incident occurred. The Security Incident Notification shall also include the date of the Security Incident Notice.
- ~~4. 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~~
5. A general description of the Security Incident, if that information is possible to determine and legally permissible to provide at the time the Security Incident Notification is provided.

5.4.2 Provider agrees to adhere to all requirements applicable to Provider providing the Services in applicable federal and state law with respect to a Security Incident related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such Security Incident.

5.4.3 Provider further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and federal and state law for responding to a Security Incident involving Student Data or any portion thereof, including Personally Identifiable Information ("**Incident Response Plan**") and agrees to provide LEA, upon request, with a summary of said written Incident Response Plan.

5.4.4 To the extent LEA determines that the Security Incident triggers third party notice requirements under applicable laws, Provider will cooperate with LEA as to the timing and content of the notices to be sent. LEA shall provide notice and facts surrounding the Security incident to the affected students, parents or guardians. Except as otherwise required by law, Provider will not provide notice of the Security Incident directly to individuals whose Personally Identifiable Information was affected, to regulatory agencies, or to other entities, without first providing written notice to LEA. This provision shall not restrict Provider's ability to provide separate security breach notification to customers, including parents and other individuals with Outside School Accounts.

5.4.5 In the event of a Security Incident originating from LEA's actions or use of the Service, or otherwise a result of LEA's actions or inactions ("**LEA Security Incident**"), Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data and may request from LEA reasonable costs incurred as a result of the LEA Security Incident.

6. INTERNATIONAL DATA PROTECTION ADDENDUM

- 6.1.** To the extent that LEA is located outside of the United States, the LEA's use of the Services will also be governed by the ClassDojo International Data Protection Addendum ("**Int. DPA**"). Please contact ClassDojo at privacy@classdojo.com to obtain the Int. DPA applicable to your jurisdiction.

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

Indirect Identifiers: Means any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty.

Personally Identifiable Information, Personal Information or PII: Means data, including Indirect Identifiers, that can be used to identify or contact a particular individual, or other data which can be reasonably linked to that data or to that individual’s specific computer or device. Student PII includes, without limitation, those items set forth in the definition of PII under FERPA. When anonymous or non-personal information is directly or indirectly linked with Personally Identifiable Information, the linked non-personal information is also treated as personal information. Persistent identifiers that are not anonymized, De-Identified or aggregated are personal information.

Program Communications: Shall mean in-app or emailed communications relating to Provider’s educational services, including prompts, messages, and content relating to the use of the Service, for example; onboarding and orientation communications, 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 Service, service updates (for example new features or content, including using for at home learning opportunities), and information about special or additional programs (e.g. ClassDojo Plus or Dojo Tutoring) offered through the Services or the ClassDojo websites or applications.

School Official: For the purposes of this DPA and pursuant to FERPA 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**” consistent with the Student Privacy Pledge, does not include a Change of Control, 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. Sell also does not include storing, sharing, transferring or disclosing Student Data with a Sub-Processor provided that the Sub-Processor does not Sell the Student Data except as necessary to perform the business purpose. Provider is also not “selling” personal information (i) if a user directs Provider to intentionally disclose Student Data or uses the Service to intentionally interact with a third party, provided that such third party also does not Sell the Student Data; or (ii) if a parent or other third party authorized by the parent lawfully acquires Student Data (e.g., enhanced classroom reports or photos) for a fee or for free.

Sub-Processor: For the purposes of this DPA, the term “Sub-Processor” means a party other than LEA or Provider, with whom Provider has a written agreement as set forth in the Standard Clauses Section 2.5, and who Provider uses for data collection, analytics, storage, or other service necessary to operate and/or improve its service, and who has access to or storage of Student Data.

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

Student Data: Student Data includes any Personally Identifiable Information, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose, 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 or identification number that would provide information about a specific student. Student Data further includes Personally Identifiable Information, as defined in 34 C.F.R. § 99.3 Education Records are Student Data for the purposes of this DPA. ~~Student Data as specified in Exhibit "B" in the Standard Schedule is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not include De-Identified Data or information that has been anonymized, or anonymous usage data regarding a student's or LEA's use of Provider's Services. Student Data shall not include information or data, including Personal Information, a student, parent, or family provides to Provider through an Outside School Account independent of the student's, parent's or family's engagement with the Services at the direction of the LEA.~~

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 website, 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 website based on the content of the web page, search query or a student's contemporaneous behavior on the website, or in response to a student's response or request for information or feedback.

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF STUDENT DATA

LEA directs Provider to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

_____Disposition is partial. The categories of Student Data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of Student Data here]

_____Disposition is Complete. Disposition extends to all categories of Student Data.

2. Nature of Disposition

_____Disposition shall be by destruction or deletion of Student Data, as set forth in Section 4.6 ("Disposition of Data"). De-Identification of Student Data shall be deemed a destruction or deletion.

_____Disposition shall be by a transfer of Student Data. The Student Data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Timing of Disposition

Student Data shall be disposed of by the following date:

_____As soon as commercially practicable

_____By *[Insert Date]*

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "E"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

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

ClassDojo Specific: Please review our Security Whitepaper for details: <https://www.classdojo.com/security/>

