Standard Student Data Privacy Agreement

IL-NDPA v1.0a

School District or LEA

Peoria County Regional Office of Education ROE 48

and

Provider

ClassDojo, Inc.

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between: Peoria County Regional Office of Education ROE 48 , located at 324 Main St Room 401 Peoria, IL 61602 (the "**Local Education Agency**" or "**LEA**") and ClassDojo, Inc. , located at 2261 Market Street STE 10437 San Francisco, CA 94114 (the "**Provider**").

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 Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

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

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

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

2. **Special Provisions.** ***Check if Required***
   - ☑ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.
   - ☑ If checked, 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 years. Exhibit E will expire 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: Danielle Lewis Title: Director of Digital Services

Address: Peoria County Courthouse, 324 Main St., Room 401, Peoria IL61602

Phone: 309-672-6906 Email: dlewis@peoriaroe.org

The designated representative for the Provider for this DPA is:

Name: Elisette Weiss Title: District Partnerships

Address: 2261 Market Street STE 10437 San Francisco, CA 94114

Phone: (707) 486-2150 Email: elisette@classdojo.com

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

LEA: Peoria County Regional Office of Education ROE 48

By: Danielle Lewis Date: 11-08-2024

Printed Name: Danielle Lewis Title/Position: Director of Digital Services

Provider: ClassDojo, Inc.

By: Elisette Weiss Date: 11/06/2024

Printed Name: Elisette Weiss Title/Position: District Partnerships

STANDARD CLAUSES
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Student Data to Be Provided**. In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

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 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

1. **Service Agreement**: ClassDojo Terms of Service located at: https://www.classdojo.com/terms/ (entered into by all individual users of LEA).

2. **Services**: Pursuant to and as fully described in the Service Agreements, Provider has agreed to provide the Services set forth below. Provider is a school communication and classroom management platform that helps bring teachers, school leaders, families, and students together. For clarity, if not opting in to use Single Sign On (SSO) or another rostering option, the LEA does not provide Student Data to Provider, rather Provider collects Student Data directly from the LEA's users and processes it on behalf of the LEA. This DPA covers access to and use of all Provider's Services, as well as any future Services that Provider may offer, unless noted below. This coverage extends, without limitation, to all subdomains, software, mobile applications, and products that are owned and operated by Provider, its subsidiaries and/or affiliates, except for those explicitly excluded below.

   Without limiting the foregoing, Provider provides the following through its platform, all of which the LEA agrees may be utilized by the LEA and its schools or users:

   - 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 users connected to an LEA classroom or school (e.g. parents or students) to disclose or share Student Data they have been provided access to by such LEA classroom or school (including, without, limitation, by teachers or other LEA employees) with third parties
   - A way for teachers, school leaders, 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
   - Optional artificial intelligence ("AI") technology-driven tools that teachers may choose to utilize
   - "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 and certain Premium Features - an optional, paid subscription or other optional paid premium features that provide additional ways for families to stay engaged with their school community and celebrate their child's growth (such as through expanded reporting on feedback points given in class, yearbooks or "Memories" products (featuring photos from Class Story, Portfolios, or School Stories). 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 ("ClassDojo Plus Non-School Use Features").

   In addition to the above, Provider may use Student Data collected from, or on behalf of, LEA, or a school within the LEA (collectively, "**education agency**"), to improve the learning experience, provide products to the education agency, and ensure secure and effective operation of Provider's products. Student Data provided by (or collected from, or on behalf of) the education agency helps provide and improve our educational products and support the education agency's and authorized users' efforts. Student Data helps Provider fulfill its duties for the purposes requested or authorized by the education agency or as otherwise permitted by applicable laws. Student Data may be used for customer support purposes, to respond to the inquiries and fulfill the requests of education agencies and their authorized users, or to enforce product access and security controls. It may be used to conduct system audits and improve protections against the misuse of our products, or to detect and prevent fraud and other harmful activities. Provider may also process Student Data for adaptive or personalized learning purposes and to provide Program Communications (as defined below) to all account holders.

   Provider Services include sharing Student Data with (i) authorized users of the Services, including parents or legal guardians and (ii) to protect the safety and integrity of users or others, or the security of the Services. ClassDojo may also use De-Identified Data for (i) product improvement and new educational product development; (ii) sharing reports on number of users, instructional time delivered or other reports on product usage and results to third parties; (iii) educational research purposes, including transferring or sharing with third parties for such purposes; and (iv) as allowed by laws.

"**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.

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

3. **Outside School Accounts:**

The Service shall not include any Outside School Accounts, Family Messaging, or Home Dojo Islands, and ClassDojo Plus Non-School Use Features. Additionally, the Service shall not include any online live tutoring services offered for children through the website located at https://tutor.classdojo.com ("**Dojo Tutor**"). Students, parents, and family users may have personal or non-school accounts (i.e., for use of the ClassDojo at home not related to school) in addition to school accounts, this includes without limitation those accounts used in connection with Provider's Family Messaging, Home Dojo Island Play, and Dojo Tutoring ("**Outside School Account(s)**"). An Outside School Account of a student may also be linked to their student account. with the Student Data elements as further detailed in the "Linked Accounts" section of the Service Agreement and as set forth here: https://classdojo.zendesk.com/hc/en-us/articles/4413231512205-What-are-Student-Accounts-and-Outside-School-Child-Accounts ("Linked Data"). 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 Linked Data or 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.

EXHIBIT "B"

SCHEDULE OF DATA

Schedule of Student Data: The following specific items or categories of Student Data may be processed by the Supplier on behalf of LEA for the purpose of the Services (collectively, the "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 Supplier 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.	X
	Other application technology meta data-Please specify: https://www.classdojo.com/cookies-policy https://classdojo.com/transparency	X
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data *Observation data about Students is optional and only collected if Teachers, School Leaders, and/or ClassDojo Admins opt to use the "Feedback Points" feature. Note this data is automatically deleted on a rolling 365-day basis.*	X
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data *Optional, only if Teacher(s) elect to record. Details here.*	X
Communications	Online communications captured (emails, blog entries) *Optional*	X
Conduct	Conduct or behavioral data *Conduct data about Students is optional and only collected if Teachers, School Leaders, and/or ClassDojo Admins opt to use the "Feedback Points" feature. Note this data is automatically deleted on a rolling 365-day basis.*	X
Demographics	Date of Birth *Optional, can be provided by either Parent or Teacher upon Student Account creation*	X
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student) *Obtained via browser/device preferences*	X
	Other demographic information-Please specify:	

Category of Data	Elements	Check if Used by Your System
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email *Optional, only if a Parent / Guardian account is created & connected to a student.*	X
	Phone *Optional, only if a Teacher invites a Parent / Guardian to connect via SMS*	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	X
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).*	X
Schedule	Student scheduled courses	
	Teacher names *Only for the classes a student is connected to, not complete schedule*	X
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	

Category of Data	Elements	Check if Used by Your System
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email *Only for Students whose teachers elect to utilize the Google Login method.*	X
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	
	Provider/App assigned student ID number	X
	Student app username	X
	Student app passwords	X
Student Name	First and/or Last *Only as provided by the Teacher(s) or School Leader(s), unless we receive it through optional SSO or Rostering features via a student information system or third-party integration like ClassLink.Initials or unique identifiers may be used.*	X
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*	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc. *Note Student Generated Content may also be teacher-assigned projects.*	X
	Other student work data -Please specify: *Note Student Generated Content may also be teacher-assigned projects.*	

Category of Data	Elements	Check if Used by Your System
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 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*	X
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

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:

[ ]

_☐_ 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 [ ]

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Peoria County Regional Office of Education ROE 48 ("Originating LEA") which is dated 11-08-2024 , 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: districts@classdojo.com.

PROVIDER: ClassDojo, Inc.

BY: _____ Date: 11/06/2024

Printed Name: Elisette Weiss Title/Position: District 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 the Peoria County Regional Office of Education ROE 48 and ClassDojo, Inc.

**PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

Subscribing LEA:

BY:_____ Date:_____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

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

***ClassDojo Specific**: Please see our Security Whitepaper for details: https://www.classdojo.com/security/*

Cybersecurity Frameworks

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 (Student Data Privacy Consortium) State Terms for Illinois**

Version IL-NDPAv1.0a (Revised March 15, 2021)

This **Exhibit G,** Supplemental SDPC State Terms for Illinois ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between Peoria County Regional Office of Education ROE 48 (the "Local Education Agency" or "LEA") and ClassDojo, Inc. (the "Provider"), is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. **Compliance with Illinois Privacy Laws.** In performing its obligations under the Agreement, the Provider shall comply with all Illinois laws and regulations pertaining to student data privacy, confidentiality, and maintenance, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/, and Local Records Act ("LRA"), 50 ILCS 205/.

2. **Definition of "Student Data."** In addition to the definition set forth in **Exhibit C,** Student Data includes any and all information concerning a student by which a student may be individually identified under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA.

3. **School Official Designation.** Pursuant to Article I, Paragraph 1 of the DPA Standard Clauses, and in accordance with FERPA, ISSRA and SOPPA, in performing its obligations under the DPA, the Provider is acting as a school official with legitimate educational interest; is performing an institutional service or function for which the LEA would otherwise use its own employees; is under the direct control of the LEA with respect to the use and maintenance of Student Data; and is using Student Data only for an authorized purpose and in furtherance of such legitimate educational interest.

4. **Limitations on Re-Disclosure.** The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. Provider will not sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena for Student Data in the possession of the Provider, the Provider shall redirect the other party to seek the data directly from the LEA. In the event the Provider is compelled to produce Student Data to another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure.

5. **Notices.** Any notice delivered pursuant to the DPA shall be deemed effective, as applicable, upon receipt as evidenced by the date of transmission indicated on the transmission material, if by e-mail; or four (4) days after mailing, if by first-class mail, postage prepaid.

6. **Parent Right to Access and Challenge Student Data.** The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or

copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105 ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any request by the LEA for Student Data in the possession of the Provider when Provider cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, no later than 5 business days from the date of the request. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data.

7. **Corrections to Factual Inaccuracies.** In the event that the LEA determines that the Provider is maintaining Student Data that contains a factual inaccuracy, and Provider cooperation is required in order to make a correction, the LEA shall notify the Provider of the factual inaccuracy and the correction to be made. No later than 90 calendar days after receiving the notice of the factual inaccuracy, the Provider shall correct the factual inaccuracy and shall provide written confirmation of the correction to the LEA.

8. **Security Standards.** The Provider shall implement and maintain commercially reasonable security procedures and practices that otherwise meet or exceed industry standards designed to protect Student Data from unauthorized access, destruction, use, modification, or disclosure, including but not limited to the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the Student Data (a "Security Breach"). For purposes of the DPA and this Exhibit G, "Security Breach" does not include the good faith acquisition of Student Data by an employee or agent of the Provider or LEA for a legitimate educational or administrative purpose of the Provider or LEA, so long as the Student Data is used solely for purposes permitted by SOPPA and other applicable law, and so long as the Student Data is restricted from further unauthorized disclosure.

9. **Security Breach Notification.** In addition to the information enumerated in Article V, Section 4(1) of the DPA Standard Clauses, any Security Breach notification provided by the Provider to the LEA shall include:

a. A list of the students whose Student Data was involved in or is reasonably believed to have been involved in the breach, if known; and

b. The name and contact information for an employee of the Provider whom parents may contact to inquire about the breach.

10. **Reimbursement of Expenses Associated with Security Breach.** In the event of a Security Breach that is attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, without regard to any limitation of liability provision otherwise agreed to between Provider and LEA, including but not limited to costs and expenses associated with:

a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;

b. Providing credit monitoring to those students whose Student Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the student's credit or financial security;

c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA

as a result of the security breach; and

d. Providing any other notifications or fulfilling any other requirements adopted by the Illinois State Board of Education or under other State or federal laws.

11. **Transfer or Deletion of Student Data.** The Provider shall review, on an annual basis, whether the Student Data it has received pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the Provider will provide written notice to the LEA as to what Student Data is no longer needed. The Provider will delete or transfer Student Data in readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within 30 calendar days if the LEA requests deletion or transfer of the Student Data and shall provide written confirmation to the LEA of such deletion or transfer. Upon termination of the Service Agreement between the Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving the request.

Any provision of Student Data to the LEA from the Provider shall be transmitted in a format readable by the LEA.

12. **Public Posting of DPA.** Pursuant to SOPPA, the LEA shall publish on its website a copy of the DPA between the Provider and the LEA, including this Exhibit G.

13. **Subcontractors.** By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom Student Data may be disclosed. This list shall, at a minimum, be updated and provided to the LEA by the beginning of each fiscal year (July 1) and at the beginning of each calendar year (January 1).

14. **DPA Term.**

a. **Original DPA.** Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be deleted, and the following shall be inserted in lieu thereof: "This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed."

b. **General Offer DPA.** The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: "The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."

15. **Termination.** Paragraph 1 of Article VII shall be deleted, and the following shall be inserted in lieu thereof: “In the event either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or been terminated. One party may terminate this DPA upon a material breach of this DPA by the other party. Upon termination of the DPA, the Service Agreement shall terminate.’

16. **Privacy Policy.** The Provider must publicly disclose material information about its collection, use, and disclosure of Student Data, including, but not limited to, publishing a terms of service agreement, privacy policy, or similar document.

17. **Minimum Data Necessary Shared.** The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider’s products and/or services is limited to the Student Data that is adequate, relevant, and limited to what is necessary in relation to the K-12 school purposes for which it is processed.

18. **Student and Parent Access.** Access by students or parents/guardians to the Provider’s programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA.

19. **Data Storage.** Provider shall store all Student Data shared under the DPA within the United States.

20. **Exhibits A and B.** The Services described in Exhibit A and the Schedule of Data in Exhibit B to the DPA satisfy the requirements in SOPPA to include a statement of the product or service being provided to the school by the Provider and a listing of the categories or types of covered information to be provided to the Provider, respectively.

EXHIBIT "H"
Additional Terms or Modifications

LEA and Provider agree to the following additional terms and modifications: The following sections shall be modified (as indicated with redlining), including any additional modifications to new changes proposed in Exhibit G by the LEA, and replaced with the language set forth below. For clarity, any changes to sections set forth in this Exhibit H shall take precedence and control over changes set forth in Exhibit G.

A. Provider Modifications to the NDPA

1. **Term:**
This DPA shall stay in effect for three years, unless and until the extent terminated by the parties. Exhibit E will expire 3 years from the date the original DPA was signed, unless and until the extent terminated by the parties.

*** Necessary to provide clarity with the termination section of the SDPC Standard Clauses.*

2. **Article II, Section 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 ~~s~~Student ~~g~~Generated ~~c~~Content to a personal account, consistent with the functionality of the ~~s~~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 Education ~~r~~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, 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.

** *Necessary to fix typos and also to reflect the reality of the Services. This also helps schools given ClassDojo has a direct relationship with users and is only for access rights nothing more.*

3. **Article II, Section 3**

Separate Account. Students, parents, and family users may have personal or non-school accounts (i.e., for use of Provider 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 as further set forth on Exhibit A ("Linked Data"). Similarly, an Outside School Account of a parent or family may be linked to their parent or family account used in school as further detailed in the "Linked Accounts" section in the Service Agreement. Student Data shall not include Linked Data or 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, ~~i~~If Student Generated Content is stored or maintained by the Provider, Provider may, ~~shall~~ at the request of the LEA, student, or student's parent or legal guardian, transfer said Student Generated Content to a separate student account or the Outside School Account; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service. In the event that Student Generated Content is transferred to the control of the student, parent or legal guardian, the copy of such Student Generated Content that is in the control of such person is no longer considered Student Data. Notwithstanding anything to the contrary, the Service shall not include any Outside School Accounts and therefore, this Agreement shall not apply to the provision of services by Provider to any person under an Outside School Account.

** *Necessary to clarify how the Services function. Additionally, FERPA and the majority of state student privacy laws (including SOPPA, Section 30) permit a parent or eligible student to request transfer of student-generated content to a personal account. Without this change, this will also impose an unnecessary burden on LEA's to respond to such requests and is likely to result in student-generated content being destroyed as upon termination to the detriment of students.*

4. Article IV, Section 6

Disposition of Data. Upon written ~~request~~ 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 ~~and~~ or according to a schedule and procedure as the Parties may reasonably agree. If the Provider has a standard retention and destruction schedule, that schedule shall apply to Student Data as long as this DPA is active. The Provider's practice relating to retention and disposition of Student Data shall be provided to the LEA upon request.

Upon termination of this DPA, ~~if no written request from the LEA is received,~~ Provider shall, unless otherwise directed by the LEA, dispose of or delete all Student Data obtained by the Provider under the Agreement within sixty (60) days of termination ~~after providing the LEA with reasonable prior notice~~ (unless otherwise required by law). If the Agreement has lapsed or is not terminated, the Student Data shall be deleted when directed or permitted by the LEA, according to Provider's standard destruction schedule, or as otherwise required by law. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or Student-Generated Content that has been transferred or kept ~~placed in a separate student account~~ pursuant to ~~s~~Section II 3. The LEA may employ a "Directive for Disposition of Data" form using Provider's standard disposition form or the form~~, a copy of which is~~ attached hereto as Exhibit "D". If the LEA and Provider employ a Provider form or 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".

** *Necessary to provide clarity if no formal request is given as well as if the Agreement has lapsed or is not formally terminated. The above language matches what is currently in NDPA v.2*

5. Article IV, Section 7

Provider is prohibited from using, disclosing, or S~~s~~elling Student Data to (a) inform, influence, or enable Targeted Advertising; (b) develop a profile of a student, family member/guardian or group, 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 the LEA, as authorized by the LEA or the parent/guardian, or as permitted by applicable law. Targeted Advertising is strictly prohibited. However, 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 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.

"Program Communications" shall have the meaning set forth in Exhibit A.

** *Necessary to provide clarity on how the Service operates and to align with NDPA v. 2 on the commercial purpose restriction.*

6. Article VII, Miscellaneous

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. With respect to the treatment of Student Data only, ~~I~~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 including as modified in this Exhibit H. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

** *Necessary to provide clarity on the various agreements*

7. Definitions

6.1 Add – The term "Sell" (first letter caps) is used in the Model Clauses, but not defined. Anywhere the term "sell" or "selling" is used, it shall be defined as set forth below.

"Sell" consistent with the Future of Privacy Forum's Student Privacy Pledge, does not include or apply to a purchase, merger or other type of acquisition of a company by another entity in which the third party assumes control of all or party of the Provider's assets, 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 sharing, transferring or disclosing Student Data with a Subprocessor that is necessary to perform a business purpose (such as detecting security incidents, debugging and repairing, analytics, storage or other processing activities) provided that the Subprocessor does not Sell the Student Data except as necessary to perform the business purpose. A sale of personal information or Student Data does not include or restrict and Provider is also not "selling" personal information or Student Data (i) if an LEA authorized user of the Services, which may include parents and legal guardians, directs Provider to intentionally disclose Student Data or uses Provider 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 user (with parent consent) acquires Student Data for free or for a fee (e.g., enhanced classroom reports, yearbooks, or photos).

6.2 Changes to the term "Student Data" as set forth below:

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 behaviour 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 (i) anonymized or ~~d~~De-~~i~~Identified, or anonymous usage data regarding a student's use of Provider's services; or (ii) any data collected from an Outside School Account (details provided in **Exhibit 'A'**).

B. Provider Modifications to the Illinois Ex. G State Supplemental Terms

1. Changes to Exhibit G, Section 1.

The following changes shall be made to Section 1 on Exhibit G:

Compliance with Illinois Privacy Laws. In performing their respective ~~its~~ obligations under the Agreement, the LEA and Provider shall comply with all Illinois laws and regulations applicable to the respective party pertaining to student data privacy and confidentiality, including but not limited to the Illinois School Student Records Act ("ISSRA"), 105 ILCS 10/, Mental Health and Developmental Disabilities Confidentiality Act ("MHDDCA"), 740 ILCS 110/, Student Online Personal Protection Act ("SOPPA"), 105 ILCS 85/, Identity Protection Act ("IPA"), 5 ILCS 179/, and Personal Information Protection Act ("PIPA"), 815 ILCS 530/ and Local Records Act ("LRA"), 50 ILCS 205/.

***Many of the laws outlined apply directly to educational institutions rather than providers. We've adjusted the language to reflect this.*

2. Changes to Exhibit G, Section 2

The following changes shall be made to Section 2 on Exhibit G:

Definition of "Student Data" In addition to the definition set forth in **Exhibit C** (as modified by Ex. H)**,** Student Data includes any and all personally identifiable information or personal information concerning a student ~~by which a student may be individually identified~~ as defined under applicable Illinois law and regulations, including but not limited to (a) "covered information," as defined in Section 5 of SOPPA (105 ILCS 85/5), (b) "school student records" as that term is defined in Section 2 of ISSRA (105 ILCS 10/2(d)) (c) "records" as that term is defined under Section 110/2 of the MHDDCA (740 ILCS 110/2), and (d) "personal information" as defined in Section 530/5 of PIPA.

3. Changes to Exhibit G, Section 4

The following changes shall be made to Section 4 on Exhibit G:

Limitations on Re-Disclosure. The Provider shall not re-disclose Student Data to any other party or affiliate without the express written permission of the LEA or pursuant to court order, unless such disclosure is otherwise permitted under SOPPA, ISSRA, FERPA, and MHDDCA. Provider will not ~~s~~Sell or rent Student Data. In the event another party, including law enforcement or a government entity, contacts the Provider with a request or subpoena forStudent Data in the possession of the Provider, the Provider shall redirect the other party to seek the datadirectly from the LEA. In the event the Provider is compelled to produce Student Data to a another party in compliance with a court order, Provider shall notify the LEA at least five (5) school days in advance of the court ordered disclosure and, upon request, provide the LEA with a copy of the court order requiring such disclosure, to the extent not otherwise prohibited by law or the court order from doing so.

***Necessary to reflect the added definition of "Sell."*

4. Changes to Exhibit G, Section 6

The following changes shall be made to Section 6 on Exhibit G:

Parent Right to Access and Challenge Student Data. The LEA shall establish reasonable procedures pursuant to which a parent, as that term is defined in 105 ILCS 10/2(g), may inspect and/or copy Student Data and/or challenge the accuracy, relevance or propriety of Student Data, pursuant to Sections 5 and 7 of ISSRA (105 ILCS 10/5; 105

ILCS 10/7) and Section 33 of SOPPA (105 ILCS 85/33). The Provider shall respond to any request by the LEA for Student Data in the possession of the Provider when Provider cooperation is required to afford a parent an opportunity to inspect and/or copy the Student Data, no later than 30 ~~5~~ business days from the date of the request. In the event that a parent contacts the Provider directly to inspect and/or copy Student Data, the Provider shall refer the parent to the LEA, which shall follow the necessary and proper procedures regarding the requested Student Data, 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.

** *Necessary to reflect the reality of the Services. This also helps schools given ClassDojo has a direct relationship with users and is only for access rights nothing more.*
** *While SOPPA outlines a 90 day response timeline for Providers, we are happy to accommodate an adjustment to 30 days.*

5. Changes to Exhibit G, Section 10

The following changes shall be made to Section 10 on Exhibit G:

Reimbursement of Expenses Associated with Security Breach. In the event of a Security Breachthat is attributable to the Provider, the Provider shall reimburse ~~and indemnify~~ the LEA for any and all costs and expenses that the LEA incurs in investigating and remediating the Security Breach, ~~without regard to any limitation of liability provision otherwise agreed to between Provider and LEA~~, including but not limited to costs and expenses associated with:

a. Providing notification to the parents of those students whose Student Data was compromised and regulatory agencies or other entities as required by law or contract;

b. Providing credit monitoring to those students whose Student Data was exposed in a mannerduring the Security Breach that a reasonable person would believe may impact the student'scredit or financial security;

c. Legal fees, audit costs, fines, and any other fees or damages imposed against the LEA as a result of the security breach; and
d. Providing any other notifications or fulfilling any other requirements adopted by the IllinoisState Board of Education or under other State or federal laws.

The Section above shall be subject to the Limitation of Liability Section set forth in the Service Agreement.

***Necessary adjustment as ClassDojo for districts is free-of-cost and, as such, we cannot provide unlimited liability. This approach aligns with SOPPA standards: the Vendor is not required to provide unlimited liability, the contract simply needs to specify how costs will be allocated.*

6. Changes to Exhibit G, Section 11

The following changes shall be made to Section 11 on Exhibit G:

Transfer or Deletion of Student Data. The LEA shall inform the Provider ~~shall review~~ on an annual basis, whether theStudent Data it has ~~received~~ requested to be processed pursuant to the DPA continues to be needed for the purpose(s) of the Service Agreement and this DPA. If, after written confirmation from the LEA, any of the Student Data is no longer needed for purposes of the Service Agreement and this DPA, the LEA ~~Provider~~ will

provide written notice to the Provider ~~LEA~~ as to what Student Data is no longer need. The Provider will delete or transfer Student Data in a readable form to the LEA, as directed by the LEA (which may be effectuated through Exhibit D of the DPA), within ~~3~~60 calendar days if LEA requests deletion or transfer of the Student Data and provide written confirmation of such deletion or transfer. Upon termination of the Service Agreement between Provider and LEA, Provider shall conduct a final review of Student Data within 60 calendar days.

If the LEA receives a request from a parent, as that term is defined in 105 ILCS 10/2(g), that Student Data being held by the Provider be deleted, the LEA shall determine whether the requested deletion would violate State and/or federal records laws. In the event such deletion would not violate State or federal records laws, the LEA shall forward the request for deletion to the Provider. The Provider shall comply with the request and delete the Student Data within a reasonable time period after receiving therequest.

Any provision of Student Data to the LEA from Provider shall be transmitted in a format readable by the LEA.

***Adjusted to align with SOPPA's expectations that LEA is responsible for informing the Provider in cases where data disposition is required.*

7. Changes to Exhibit G, Section 13

The following changes shall be made to Section 13 on Exhibit G:

Subcontractors. By no later than (5) business days after the date of execution of the DPA, the Provider shall provide the LEA with a list of any subcontractors to whom Student Data may be disclosed or a link to a page on the Provider's website that clearly lists any and all subcontractors to whom StudentData may be disclosed. LEA acknowledges that Provider has done so by providing the link set forth in the Schedule of Data on Exhibit B ("Service Provider List"). This list shall, at a minimum, be updated ~~and provided to the LEA~~ by the beginningof each fiscal year (July 1) and at the beginning of each calendar year (January 1).

***This list can be accessed at any time via this link: https://www.classdojo.com/third-party-service-providers/*

8. Changes to Exhibit G, Section 14

The following changes shall be made to Section 14 on Exhibit G:

DPA Term.

a. **Original DPA.** Paragraph 4 on page 2 of the DPA setting a three-year term for the DPA shall be deleted, and the following shall be inserted in lieu thereof: "This DPA shall be effective upon the date of signature by Provider and LEA, and shall remain in effect as between Provider and LEA 1) for so long as the Services are being provided to the LEA or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first. ~~The Exhibit E General Offer will expire three (3) years from the date the original DPA was signed~~."

b. **General Offer DPA.** The following shall be inserted as a new second sentence in Paragraph 1 of Exhibit E: "The provisions of the original DPA offered by Provider and accepted by Subscribing LEA pursuant to this Exhibit E shall remain in effect as between Provider and Subscribing LEA 1) for so long as the Services are being provided to Subscribing LEA, or 2) until the DPA is terminated pursuant to Section 15 of this Exhibit G, whichever comes first."

***Necessary to remove the conflicting language as-written in Sections 14.a and 14.b.*

9. Changes to Exhibit G, Section 17

The following changes shall be made to Section 17 on Exhibit G:

Minimum Data Necessary Shared. The Provider attests that the Student Data request by the Provider from the LEA in order for the LEA to access the Provider's products and/or services is limited to the Student Data that is ~~adequate, relevant, and~~ limited to what is reasonably necessary in relation to the K-12 school purposes for which it is processed and for the purposes set forth on Exhibit A.

10. Changes to Exhibit G, Section 18

The following changes shall be made to Section 18 on Exhibit G:

Student and Parent Access. Access by students or parents/guardians to the Provider's programs or services governed by the DPA or to any Student Data stored by Provider shall not be conditioned upon agreement by the parents/guardians to waive any of the student data confidentiality restrictions or a lessening of any of the confidentiality or privacy requirements contained in this DPA. The foregoing shall not apply to any parent provided consent to link Student Data to an Outside School Account, including the Linked Data.

11. Changes to Exhibit G, Section 19

The following changes shall be made to Section 19 on Exhibit G:

Data Storage. Provider shall store all Student Data shared under the DPA within the United States, unless otherwise noted in Provider's Service Provider List.

Signature Certificate

Reference number: HUTF9-D3VCX-QNX4S-H2N2A

Signer	Timestamp	Signature
Danielle Lewis Email: dlewis@peoriaroe.org		
Sent:	08 Nov 2024 23:02:59 UTC	
Viewed:	08 Nov 2024 23:56:43 UTC	
Signed:	08 Nov 2024 23:59:13 UTC	
Recipient Verification:		IP address: 64.6.3.214
✔Email verified	08 Nov 2024 23:56:43 UTC	Location: Macomb, United States

Document completed by all parties on:
08 Nov 2024 23:59:13 UTC