STANDARD STUDENT DATA PRIVACY AGREEMENT

TX-NDPA v1r6

Manor Independent School District
and
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:

and [Manor Independent School District], located at [10335 US HWY 290 E, Manor, TX 78653] (the "**Local Education Agency**" or "**LEA**")

ClassDojo, Inc., located at 735 Tehama Street, San Francisco, CA 94103 (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 Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

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

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

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

2. **Special Provisions.** ***Check if Required***

   ☑ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   ☑ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H". (Optional)**

   ☑ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

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

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

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

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

The designated representative for the LEA for this DPA is:

Name: Moises Hernandez Santiago Title: CFO

Address: 10335 US Hwy 290E Manor TX 78653 -

Phone: 1 (512) 278-4000

Email: moises.hernandezsantiago@manorisd.net

The designated representative for the Provider for this DPA is:

Name: Jeff Buening Title: General Manager, District Partnerships

Address: 735 Tehama Street, San Francisco, CA 94103

Phone: 513-720-094 Email: jeff.buening@classdojo.com

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

LEA:

Signed by:

By: Moises Hernandez Santiago Date: 1/31/2026 | 9:03 PM PST

ED2CD6295D3E4B9...

Printed Name: Moises Hernandez Santiago Title/Position: CFO

Provider:

Signed by:

By: Jeff Buening Date: 1/30/2026 | 6:47 PM PST

28F6E5F8C1024EF...

Printed Name: Jeff Buening Title/Position: General Manager, 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 the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

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

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

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

2. **Parent Access**. To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests**. Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws**. LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use**. The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. **Provider Employee Obligation**. Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect

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

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

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

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

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

ARTICLE V: DATA PROVISIONS

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

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

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

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

   (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

      i. The name and contact information of the reporting LEA subject to this section.

      ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

      iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

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

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

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

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

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

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

ARTICLE VI: GENERAL OFFER OF TERMS

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

ARTICLE VII: MISCELLANEOUS

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

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

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

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

4. **Entire Agreement**. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound**: This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

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

EXHIBIT "A"

DESCRIPTION OF SERVICES

STANDARD SCHEDULE

1. **Service Agreement**: The ClassDojo District Terms of Service are located at https: https://www.classdojo.com/district-terms ("ClassDojo District Terms"). The ClassDojo District Terms incorporate by reference additional terms entered into by both LEA and all individual users of the Service, located at: https://www.classdojo.com/terms ("ClassDojo Terms of Service"). The ClassDojo District Terms and ClassDojo Terms of Service are collectively the "Service Agreement". This DPA is hereby incorporated by reference into the Service Agreement.

2. **Services**: Pursuant to and as fully described in the Service Agreement, 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 ("Rostering"), 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. In addition, even if utilizing Rostering, LEA users will still input Student Data and other information directly into the Services. This DPA covers access to and use of all Provider's Services, as well as any future Services that Provider may offer as added pursuant to Article I, Section 1.2 of the DPA, 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 where teachers are not included ("Family Chat") or parent-to-parent groups or "social networks" with various digital communication features where a teacher is not included ("Family Communities") are not part of the Services
   - Classroom Management Tools: Features that allow teachers, school leaders and administrators to give feedback points and assignments to students, and other classroom management tools (e.g. attendance).
   - A way for teachers to share photos, videos, files, and more from the classroom for families and students to see, including on Class Stories and School Stories. School Stories and Class Stories also includes the ability for teachers, school leaders, families and students to post comments and "likes" on the Class Stories and School Stories.
   - A way for users connected to an LEA classroom or school (e.g. parents/families 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.
   - Student Portfolios: Includes the ability of students to share their classroom 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 ("AI Classroom Tools"). For more information please see: https://ai.classdojo.com/. Teachers may choose to utilize certain AI Classroom Tools to save time and create more personalized comments. In addition, ClassDojo may provide certain AI features to assist teachers, school leaders and administrator with certain non-classroom related use tasks (e.g. uploading rostering lists) ("AI Productivity Tools"). These users may choose to provide "inputs" that may contain text or photos/videos (e.g., a photo of a class list of students) in connection with the use of these AI Productivity Tools. Please see our AI Transparency Page located at: https://www.classdojo.com/ai-tools-transparency-note/ for more details. ClassDojo also provides certain AI technology tools for use by parents at home (e.g. generating a coloring page based on the child's interests) that are not considered part of the Services ("Parent AI Tools").
   - "Class 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 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 Stories, 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, Dojo Sparks (a learn-to-read program designed for at-home use) and Learning tab content and activities that the parties agree are not part of the Services ("ClassDojo Plus Non-School Use Features").
- ClassDojo for Districts: A centralized dashboard for managing optional staff rostering and SSO information, retrieving messaging records, district-level announcements and messaging, analytics on each school's adoption and feature usage, and accessing ClassDojo customer support at the district level. School leaders and certain District users will be able to view this. Districts may separately enter into a District Master Service Agreement with Provider.
- Dojo Tutor in Schools: Certain Dojo Tutor (as defined below) information, such as tutor assessments, feedback, and other session information (e.g. session recordings) ("Dojo Tutor Information") may be shared at the direction of the parent to their child's teacher with the parent's approval to the main ClassDojo Services ("Dojo Tutor Information Sharing"). When this Dojo Tutor Information Sharing occurs with the ClassDojo Services, a copy of the Dojo Tutor Information will be made to share. This is a copy of the assessment and only this copy will become Student Data once the teacher has elected to save and bring this information into either their account or the student's account in the Services ("Student Account"). The child's Student Account information on ClassDojo will remain separate, ensuring that school information remains segregated and separate from non-school information. For more information, please see our FAQ located here: https://help.classdojo.com/hc/en-us/articles/4413231512205-What-are-Student-Accounts-and-Outside-School-Child-Accounts. While Dojo Tutor may match the teacher's first and last name, school information, and email address from an existing in-school Services account to enable the Dojo Tutor Information to be shared, Dojo Tutor will not make this Dojo Tutor Information downloadable to the teacher or accessible in any in-school ClassDojo account unless the Dojo Tutor Information was shared at the direction of (or by) the parent, nor will it treat such Dojo Tutor Information as an Education Record or Student Data under the Family Educational Rights and Privacy Act of 1974 ("**FERPA**") until such time as Dojo Tutor has entered into a contractual relationship to provide such Dojo Tutor Services to the school or district.

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 (as allowed by law) 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).

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 and Linked Data:**

(a) Outside School Accounts: The Service shall not include any Outside School Accounts (as defined below) and those products and features set forth in 3(b) of this Exhibit "A" and therefor this DPA shall not apply to the provisions of services by Provider to any person under an Outside School Account. Additionally, the Service shall not include any online live tutoring services offered for children through the website located at https://tutor.classdojo.com/ or any associated mobile applications ("**Dojo Tutor**"). Students, parent, 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 with the Student Data elements as further set forth below **("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 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. 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, or upon request by the parent or student; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service.

Linked Data: The Parties agree that an Outside School Account of a student may also be linked to their Student Account with the Linked Data containing the Student Data elements as further described in the "Linked Accounts" section of the Service Agreement and set forth here: https://classdojo.zendesk.com/hc/en-us/articles/4413231512205-What-are-Student-Accounts-and-Outside-School-Child-Account. The Parties further agree that Linked Data is not subject to the requirements found in Section 4.8 (Disposition of Data) of the DPA.

(b) The following non-school services and data are excluded (except as noted below) from the Services provided to the LEA and shall not be considered covered by this DPA:

- Family Chat
- Family Communities
- Home Island
- ClassDojo Plus Non-School Use Features
- Parent AI Tools
- Dojo Tutor - except for certain Dojo Tutor Information when specifically shared at the direction of the parent or any Dojo Tutor services to be contracted to be part of the Services
- Linked Data - to be used in both the school Services and the Outside School Account
- Parent Account Data - to be used in both the school Services and Outside School Account as noted in Section 4 of this Exhibit "A"

4. Provider Use of Account Data as a Controller

The Parties agree that Provider shall use certain limited Account Data (as defined below) collected in connection with the Services as a "controller" as that term is defined in applicable privacy laws, or if not defined means the entity which determines alone or jointly with others the purposes and means of the processing of Personal Information. For clarity, this means that Provider will not be a "service provider" or "school official" with respect to the Account Data.

"**Account Data**" means information that LEA or LEA's end users provide directly to Provider in connection with the creation or administration of its Provider account, such as name, screen name, email address, school and class affiliation of a parent, and password of an LEA or an LEA end user (e.g., a parent or teacher) but shall otherwise exclude LEA's end user data as well as any student registration data.

Provider may process Account Data, as an independent controller, for one of the following exhaustive list of purposes:

(i) Billing, account, and LEA and LEA end user relationship management and related end user correspondence (e.g., mailings about necessary updates and product capabilities);

(ii) Complying with and resolving legal obligations, including responding to data subject requests for Personal Information processed by Provider as a controller, tax requirements, online safety and content moderation requirements (including making notifications to law enforcement where required by law), agreements and disputes, and enforcing Provider’s rights; and

(iii) Any Family Chat and Family Communities as defined above.

EXHIBIT "B"

SCHEDULE OF 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. *Note this data is automatically deleted on a rolling 365-day basis.*
	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. *Note, Family Messaging is not considered Student Data.*
Biometric Data	Physical or behavioral human characteristics that can be used to identity a person (e.g. fingerprint scan, facial recognition)	N/A from students; may use to validate parents/teachers with iOS or Android technology – ClassDojo is 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. Note this data is automatically deleted on a rolling 365-day basis.

Demographics	Date of Birth	✓
	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)	N/A *We do obtain browser/device language preferences, though this does not indicate native or primary language spoken by student.*
	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)	N/A *We track product events and progress within a particular feature, not grade or performance of an assignment*
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 Page (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 Subprocessors: https://www.classdojo.com/third-party service-providers/

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 termsof 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 Provider Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Manor Independent School District ("Originating LEA") which is dated [1/30/2026 | 6:47 PM PST], 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: **dpa@classdojo.com**

ClassDojo

Signed by:

BY: Jeff Buening Date: 1/30/2026 | 6:47 PM PST

28F6E5F8C1024EF...

Printed Name: Jeff Buening Title/Position: General Manager – District Partnership

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 [**Insert Name of Originating LEA**] and the Provider. **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 .

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 State Terms for Texas

Version 1.0

This **Exhibit "G"**, Supplemental SDPC State Terms for Texas ("Supplemental State Terms"), effective simultaneously with the attached Student Data Privacy Agreement ("DPA") by and between [Manor Independent School District] (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. **Covered Data.** All instances of "Student Data" should be replaced with "LEA Data". The protections provided within this DPA extend to all data provided to or collected by the Provider.

2. **Compliance with Texas Privacy Laws and Regulations.** In performing their respective obligations under the Agreement, the LEA and the Provider shall comply with all Texas laws and regulations pertaining to LEA data privacy and confidentiality, including but not limited to the Texas Education Code Chapter 32, and Texas Government Code Chapter 560.

3. **Modification to Article III, Section 2 of the DPA.** Article III, Section 2 of the DPA (Annual Notification of Rights.) is amended as follows:

   ~~**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.~~
   Consider Provider as School Official. The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records received from the LEA pursuant to the DPA. For purposes of the Service Agreement and this DPA, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from the education records received from the LEA.

4. **Modification to Article V, Section 4 of the DPA.** Article V, Section 4 of the DPA (Data Breach.) is amended with the following additions: (6) For purposes of defining an unauthorized disclosure or security breach, this definition specifically includes meanings assigned by Texas law, including applicable provisions in the Texas Education Code and Texas Business and Commerce Code. (7) The LEA may immediately terminate the Service Agreement if the LEA determines the Provider has breached a material term of this DPA. (8) The Provider's obligations shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

5. **Modification to Article VII, Section 4 of the DPA.** Article VI, Section 4 of the DPA (Annual Notification of Rights.) is amended as follows:

   Entire Agreement. This DPA ~~and the Service Agreement~~ constitutes 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.

6. **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, including but not limited to costs and expenses associated with:

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

   b. Providing credit monitoring to those employees or students whose LEA Data was exposed in a manner during the Security Breach that a reasonable person would believe may impact the employee’s or 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 Texas State Board of Education, Texas Education Agency, or under other State or federal laws.

7. **No Exhibit E without unaltered DPA including Texas Addendum.** Any alterations are only allowed in **Exhibit “H”**. Any terms under **Exhibit “H”** do not apply to **Exhibit “E”** and render **Exhibit “E”** null and void.

EXHIBIT "H"

Additional Terms or Modifications

Version

LEA and Provider agree to the following additional terms and modifications, and the following sections shall be modified (as indicated) and replaced with the language set forth below.

:

ARTICLE V: DATA PROVISIONS

LEA and Provider agree to the following additional terms and modifications: The following sections shall be

modified (as indicated) and replace with the language set forth below.

Ex. G Modifications:

~~**Covered Data.** All instances of "Student Data" should be replaced with "LEA Data". The protections provided within this DPA extend to all data provided to or collected by the Provider.~~

*****Reason for change: "Covered Data" is a defined term, and does not include other types of data that the LEA may provide. This DPA provides for the protection of Student Data (as defined herein) and is not meant to cover all of the data that is provided to or collected by Provider.***

Entire Agreement. This DPA and the Service Agreement constitute~~s~~ 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.

*****Reason for change: the SDPA contemplates that a Service Agreement – which includes necessary commercial terms – is included in the "Entire Agreement" between the parties.***

Reimbursement of Expenses Associated with Security Breach. Subject to the exclusions and limitation of liability set forth in the Service Agreement, ~~I~~in the event of a Security Breach that is solely attributable to the Provider, the Provider shall reimburse and indemnify the LEA for any and all reasonable costs and expenses that the LEA incurs in investigating and remediating the Security Breach, including but not limited to costs and expenses associated with:

a. Providing notification to ~~the employees or parents of those students~~individuals whose ~~LEA Data~~ Personally Identifiable Information was compromised and regulatory agencies or other entities as required by law or contract if required by applicable law;

b. Providing credit monitoring to those ~~employees or students~~individuals whose ~~LEA Data~~Personally Identifiable Information was exposed in a manner during the Security Breach that a reasonable person would believe may impact the ~~employee's or student's~~individual's credit or financial security if required by applicable law;

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 applicable to the Service provided by Contractor and adopted by the Texas State Board of Education, Texas Education Agency, or under other State or federal laws.

****Reason for change: necessary to incorporate reference to the Service Agreement terms and to make clear that these obligations apply to the extent required by applicable law.***

1. Recitals:

Changes to the Recitals Section as indicated below:

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.~~attached Exhibit "A" ("Standard Schedule").

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.~~Reserved.

4. ~~This DPA shall stay in effect for three (3) years. **Exhibit "E"** will expire three (3) years from the date the original DPA was signed.~~ Term and Termination. In the event that either Party seeks to terminate this DPA, they may do so by written notice if 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. This DPA shall stay in effect for as long as the Provider retains the Student Data, as set forth in section Article IV, Section 4.6, Disposition of Data. In the case of a "Change of Control" the LEA has the authority to terminate the DPA if it reasonably believes that the successor cannot uphold the terms and conditions herein or having a contract with the successor would violate the LEA's policies or state or federal law.

****Reasons for changes: To specify location of Standard Schedule, to remove duplicative terms, and to specify the Term of the DPA and to address Termination events.***

The following new sections are added to the Recitals Section:

7. **Data Disposition on Service Agreement 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 4.6 of the Standard Clauses.

8. **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.

**** Reason for changes: necessary to provide clarity with the termination section of the SDPC Standard Clauses, to reference Data Disposition requirements, and to permit execution of this Agreement via electronic signature.***

2. Article I: Purpose and Scope

Changes to Section 1.3 as indicated below:

1.3 Student Data to Be Provided. In order to perform the Services described above, ~~LEA shall provide~~ Provider shall process Student Data as identified in the Schedule of Data, attached hereto as Exhibit "B". Student Data may be provided by the LEA or created by students, as set forth fully in the definition of Student Data in Exhibit "C". If a Provider needs to update any information on Schedule of Data set forth in the Standard Schedule, they may do so by completing the Exhibit Addendum and sending a copy to the LEA.

Provider may delete data elements from the Schedule of Data if they are no longer used by the Provider. Provider must add data elements to the Schedule of Data, when a material change has occurred, regardless of whether the added data elements are either one of the following:

1. used to better deliver the original products or services listed in the DPA, or

2. used to deliver added products or services that result in new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed. Such new products or services must be designated in the Exhibit Addendum as changes to Exhibit "A".

The Provider must notify the LEA, in accordance with the notification provisions of this DPA, of the existence and contents of an Exhibit Addendum modifying the Schedule of Data. The LEA will have thirty (30) days from receipt to object to the Exhibit Addendum. If no written objection is received it will become incorporated into the DPA between the parties.

****Reason for changes: necessary to specify in more detail the Student Data to be provided and to include a description of the process to allow for updates to be made to the Schedule of Data.***

A new Section 1.5 is added after Section 1.4 as follows:

Description of Products and Services. A description of all products and services covered by the Agreement, and information specific to this DPA, are listed in Exhibit "A". If a Provider needs to update any information on Exhibit "A" (such as updating with new provided services), they may do so by completing an addendum and sending a copy to the LEA ("Exhibit Addendum"). Provider may add or delete products or services subject to this DPA under the following circumstances:

1. Deleted products or services: The products or services have been discontinued and are no longer available from the Provider.

2. Added products or services: The added products or services are either:

a. a direct replacement, or substantially equivalent to the original products or services listed in the DPA, or

b. the added products or services result in enriched new or enhanced capabilities, new modules, technology advancements and or service categories relating to the listed products or services that Provider did not have at the time the DPA was signed.

If an added product or service requires additional Data Elements, Provider must complete the relevant portion of the Exhibit Addendum template to update the Schedule of Data.

Provider may not make any change to Exhibit “A” via an Exhibit Addendum, except adding or deleting products or services. LEA is under no obligation to acquire added products or services, and has no ability under the DPA to prevent deletion of products or services. Subject to the limitations in this section, an Exhibit Addendum modifying Exhibit “A” is automatically incorporated into this DPA when LEA is notified by Provider, in accordance with the notification provisions of this DPA, of the Exhibit Addendum’s existence and contents.

Reason for changes: necessary to address products and services being offered and how products and services may change.

3. Article II: Data Ownership and Authorized Access

Changes to Section 2.1 as indicated below:

1. Student Data Property of LEA. As between LEA and Provider, ~~A~~all Student Data ~~transmitted to~~processed by 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~~processed by the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA or the party who provided such data (such as the student or parent). ~~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.~~

Reason for changes: necessary to delineate property rights and to remove duplicate terms.

Changes to Section 2.2 as indicated below:

2. Parent, Legal Guardians and Student 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.

2.2.1 This NDPA does not impede the ability of students, or student’s parent or legal guardian to download, export, transfer, or otherwise save or maintain their own Student Generated Content directly from Provider or for Provider to provide a mechanism for such download, export, transfer or saving to students, or the student's parent or legal guardian. Nor does it impede the ability of Providers to offer LEAs features to allow such ability.

~~2.2.1~~2.2.2 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.

** ***Reason for changes: necessary to reflect the functioning of the Services and to make the language on Student Generated Content consistent within Section 2.2 with respect to parents and guardians. This also helps schools given ClassDojo has a direct relationship with users and is only for access rights. Without this direct parent to Provider access request process, LEAs must create and staff a process to collect the parent access request and then will need to send the access request back to the Provider to respond anyway, given LEA does not have the direct ability to provide the Student Data collected from the Services directly to the parents.***

Replace Section 2.3 with the language indicated below:

2.3 Outside School Account. Students, parent, 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 with the Student Data elements as further described in **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. 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. Notwithstanding anything to the contrary, the Service shall not include the Outside School Accounts and therefore this DPA shall not apply to the provision of services by Provider to any person under an Outside School Account. 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, or upon request by the parent or student; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service. Linked Data shall not be subject to Section 4.6 (Disposition of Data).

** ***Reason for changes: Replacement of Section 2.3 is necessary to clarify how the Services function.***

Changes to Section 2.4 as indicated below:

2.4 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 Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA. Every Subprocessor Agreement must provide that the Subprocessor will not Sell the Student Data. The terms of a Subprocessor Agreement shall not be materially modified by the Subprocessor unless notice is provided to the Provider. The list of Provider's current Subprocessors can be accessed through the Provider's Privacy Policy (which may be updated from time to time).

*****Reason for changes: Necessary to address additional restrictions on Subprocessors and to provide direction as to where information about Provider's Subprocessors can be found.***

4. Article III: Duties of LEA

Changes to Section 3.2 as indicated below:

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 S~~s~~chool O~~o~~fficial 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 Subprocessors 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.

*****Reason for changes: necessary to clarify LEA duties with respect to rights notification under applicable law.***

Changes to Section 3.4 as indicated below:

3.4 Unauthorized Access Notification. LEA shall notify Provider promptly (but within 72 hours) of any ~~known unauthorized access~~confirmed Data Breach to the Services, LEA's account or any Student Data that poses a privacy or security risk. If requested by Provider, LEA will assist Provider in any efforts by Provider to investigate and respond to ~~any unauthorized access~~such Data Breach.

*****Reason for changes: necessary to delineate LEA duties in case of a Data Breach.***

5. Article IV: Duties of Provider

Changes and additions to Section 4.4 as indicated below:

4.4 No Disclosure. Provider acknowledges and agrees that it shall not ~~make any re-disclosure of~~Sell or disclose any Student Data or any portion thereof, including without limitation, user content or other nonpublic 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.~~

4.4.1 Exceptions to No Disclosure.

4.4.1.1 The prohibition against disclosure will not apply to Student Data where the disclosure is directed or permitted by the LEA or this Agreement.

4.4.1.2 This provision to not Sell Student Data shall not apply to a Change of Control.

4.4.1.3 This prohibition against disclosure shall not apply to Student Data disclosed pursuant to a judicial order or lawfully issued subpoena, warrant or other legal process. This prohibition against disclosure shall not apply to Student Data disclosed to Subprocessors performing services on behalf of the Provider pursuant to this DPA.

4.4.1.4 Should law enforcement or other government entities ("Requesting Party(ies)") provide a judicial order or lawfully issued subpoena or warrant to the 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.

4.4.1.5 Notification under 4.4.1.5 is not required if the judicial order of lawfully issued subpoena or warrant states not to inform the LEA of the request, or if the Provider is otherwise legally prohibited.

4.4.1.6 Should the LEA be presented with a judicial order or lawfully issued subpoena or warrant to disclose Student Generated Content or other Student Data, the Provider shall cooperate with the LEA in delivering such data.

4.4.1.7 This prohibition against disclosure shall not apply to LEA authorized users of the Services, which may include parents or legal guardians.

4.4.1.8 This prohibition against disclosure shall not apply to protect the safety of users or others.

4.4.1.9 This prohibition against disclosure shall not apply to protect the integrity or the security of the Services. 4.4.1.10 This prohibition against disclosure shall not apply to De-Identified information.

**** *Reason for changes: Necessary to maintain consistency with applicable state student privacy laws and to clarify the permitted exceptions to the prohibition on disclosure.***

Changes to Section 4.5 as indicated below:

De-Identified Data: Provider agrees not to attempt to re-identify de-identified Student Data without the written direction of the LEA. De- Identified Data may be used by the Provider for those purposes allowed under applicable laws, for the purposes allowed for the processing of Student Data under this DPA,~~FERPA and~~ as well as the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development and improvement of the Provider's educational sites, ~~s~~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 Student 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. If Provider chooses to create De-Identified Data, its process must comply with either NIST de-identification standards or US Department of Education guidance on de-identification.

***** Reason for changes: Necessary to maintain consistency with FERPA and state student privacy laws related to the disclosure of De-Identified Data. In addition, the changes with respect to Subprocessors is to match the language set forth in Section 2.4 "Subprocessors".***

6. Article IV: DUTIES OF PROVIDER

Changes to Section 4.6 as set forth below:

Disposition of Data: Upon written request 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 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~~unless otherwise directed by the LEA, Provider shall dispose of or delete all Student Data obtained by the Provider under the ~~Service~~ Agreement within sixty (60) days of termination (unless otherwise required by law). If the Agreement has lapsed or is not terminated, the Student Data shall be deleted (a) when directed or permitted by the LEA, (b) according to Provider's standard destruction schedule, or (c) as otherwise required by law~~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, Student-Generated Content that has been transferred or kept pursuant to Section 2.2.2, or Linked Data. or placed in an Outside School Account~~ 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.

*****Reason for Changes: Necessary to address circumstances when Provider has a standard retention and destruction schedule and to address data deletion when the Agreement has lapsed or has not terminated. This also clarifies that these deletion terms do not apply to data transferred to Outside School Accounts and Linked Data.***

Changes to Section 4.7 as set forth below:

Advertising Limits. Provider is prohibited from using, disclosing, or ~~s~~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 or as authorized by the parent or legal guardian; or (c) for any commercial purpose other than to provide (which shall include maintaining, developing, supporting, improving, and diagnosing) the Service to the LEA, as authorized by the designated representative for 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 for employment, school, educational or other learning purposes within a school service when such recommendation is not determined in whole or part by payment or other consideration from a third party ~~to teachers or LEA employees~~; or (iii) to notify student users about Service updates or new features that do not substantially alter the Service and that are not Targeted Advertising; or (iv) to notify non-Student account holders about new education product updates, features, or services or~~-~~; (v) from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

** ***Reason for changes: Necessary to better align with state student privacy laws and also to provide clarification on permitted use of Student Data.***

7. Article V, Data Provisions

Changes to Section 5.2 as indicated below:

Audits. No more than once a year, or following ~~unauthorized access~~a Data Breach, 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, ~~T~~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~~the LEA, as reasonably necessary to fulfill the requests of such Security Audit. ~~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.~~

Costs for the Security Audit are the responsibility of the LEA. Alternatively, Provider may provide an independent third-~~-~~party report in place of allowing LEA to conduct such Security Audit. Provider may redact the independent third-~~-~~party report to protect information, security, intellectual property and privacy.

*****Reason for changes: Necessary to align terms with the definition of Security Breach and to address audit costs, and alternatives to an audit.***

Changes to Section 5.4 as indicated below:

Data Breach. In the event that Provider confirms a Data Breach, ~~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 as required by applicable state law, but in no event later than ~~within~~ seventy-two (72) hours of confirmation of the ~~incident~~Data Breach (“Data Breach Notification”), unless notification within this time limit would disrupt investigation of the ~~incident~~ Data Breach by either the Provider or by law enforcement. In such an event, Data Breach ~~n~~Notification shall be made within a reasonable time after discovery of the ~~incident~~Data Breach. A Data Breach 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:

(1) Unless otherwise required by applicable state law, ~~T~~the ~~security~~ Data ~~b~~Breach ~~n~~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~~Provider subject to this section.

ii. A ~~list~~ description of the ~~types of personal information~~Student Data ~~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 Data ~~b~~Breach, (2) the estimated date of the Data ~~b~~Breach, or (3) the date range within which the Data ~~breach~~ 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,~~ Data Breach, if that information is possible to determine at the time the ~~notice~~ Data Breach Notification is provided.

vi. Identification of impacted individuals.

(2) Provider agrees to adhere to all federal and state requirements applicable to Provider with respect to a D~~d~~ata B~~b~~reach ~~related~~ to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such D~~d~~ata B~~b~~reach.

(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 D~~d~~ata B~~b~~reach~~, breach of security, privacy incident or unauthorized acquisition or use of~~ involving Student Data or any portion thereof (“Incident Response Plan”), ~~including personally identifiable information and~~ agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) To the extent LEA determines that the Data Breach 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 Data Breach incident to the affected students, parents or guardians. Except as otherwise required by law, Provider will not provide notice of the Data Breach 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. ~~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 actions or use of the Service, or otherwise a result of LEA's actions or inactions, ("Lea Security Incident"), Provider shall reasonably cooperate with LEA to the extent necessary to expeditiously secure Student Data and may request from LEA costs incurred as a result of the LEA Security Incident.

*****Reason for changes: Necessary to align with applicable law, to clarify each party's respective roles and responsibilities in the event of a Data Breach.***

8. 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. 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.

*****Reason for changes: Necessary to provide clarity on precedence of the various documents.***

9. Definitions.

Add or change the following terms:

Change of Control: Any merger, acquisition, consolidation, or other business reorganization or sale or all or substantially all of the assets of Provider or of the portion of Provider that performs the Services in the Service Agreement.

Contextual Advertising: Contextual advertising is the delivery of advertisements based upon a current visit to a Web page or a single search query, without the collection and retention of data about the consumer's online activities over time.

Data Breach: A confirmed unauthorized release, access to, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider in violation of applicable state or federal law.

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~~.

Directory Information Exemption: For the purposes of this DPA, the "Directory Information Exemption" means the exemption under FERPA set forth in 34 CFR § 99.3 and 34 CFR § 99.37.

Education~~al~~ Records: Education~~al~~ Records shall have the meaning set forth under FERPA cited as 20 U.S.C. 1232 g(a)(4). For additional context see also the Student Data definition. ~~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.~~

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.

~~**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.~~

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 or Student Data.

Personally Identifiable Information. Personal Information or PII: Means any information, including Indirect Identifiers, that is linked or that can be reasonably linked to an identified or identifiable person or to that individual's specific computer or device. When anonymous or non-personal information is directly or indirectly linked with Personal 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.

~~**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.~~

"**Sell**" consistent with the Future of Privacy's Student Privacy Pledge, does not include or apply to a purchase, merger or other type of acquisition of a company by another entity, provided that the company or successor entity continues to treat the Personally Identifiable Information contained in Student Data in a manner consistent with this DPA with respect to the previously acquired Personally Identifiable Information contained in Student Data. Sell also does not include sharing, transferring or disclosing Student Data with a Service Provider 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 Service Provider 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 ClassDojo 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) purchases Student Data (e.g., enhanced classroom reports or photos).

School Official Exemption: For the purposes of this DPA, the “School Official Exemption” means the exemption set forth under FERPA Section 34 CFR§ 99.33(a)(1) and 99.7 (a)(3)(iii).

Student Data: Student Data includes any Personally Identifiable Information, ~~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 E~~e~~ducational R~~r~~ecord 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 Metad~~ D~~ata that has not been stripped of all direct and indirect identifiers. Student Data further includes “P~~p~~ersonally I~~i~~dentifiable I~~i~~nformation (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~~ include Student-Generated Content or De-Identified Data ~~that~~ or information that has been anonymized or de-identified, or anonymous usage data regarding a student’s or LEA’s use of Provider’s services. Student Data shall also not include (i) 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; and (ii) Linked 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 Generated Content” does not include student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment

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~~ Contextual Advertising, 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."~~

***Reason for changes**: New definitions are necessary to reflect the way Provider's Services operate, including with respect to Outside School Accounts and Linked Data. Additional changes to clarify what qualifies as Personally Identifiable Information to match state student privacy laws and with respect to Student-Generated Content to match Article II, Section 2.2.2. Adding additional changes to match definitions in state student privacy laws.*

10. Definitions. Any defined term used in the Agreement and in Exhibit G shall be shown as first letter capitalized.

**** Reason for changes: To the extent there are any defined terms that are not shown with first letter capitalization, this is needed to provide clarity for the parties. With respect to the defined term "Services" this shall only be first letter capitalized where such term is meant to refer to the Provider Services as set forth in Ex. A, not "services" as that term is used generally. References to Operator, Provider or a Third Party are not necessary, as "Provider" is identified on the first page of the DPA.***

Removed: ~~Data Breach~~

(1) ~~In the event of a breach arising from Provider's intentional misconduct or negligence, Provider agrees to indemnify the LEA from and against any and all claims brought by a parent and/or student for damages from such a breach, to include any costs of defense to litigation.~~

Reason for change: Indemnification obligations are addressed in the Service Agreement.

11. Exhibit G to this DPA: Section 7 (No Exhibit E without unaltered DPA including Texas Addendum) is deleted in its entirety.

*****Reason for changes: Necessary to maintain a valid Exhibit E for other LEAs to execute as needed.***