

STANDARD STUDENT DATA PRIVACY AGREEMENT

**MASSACHUSETTS, MAINE, IOWA, MISSOURI, NEBRASKA,
NEW JERSEY, OHIO, RHODE ISLAND, TENNESSEE, VERMONT, AND VIRGINIA**

MA-ME- IA-MO-NE- NJ -OH-RI-TN-VT-VA-DPA, Modified Version 1.0

Norton City Schools

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: Norton City Schools, located at 4128 S Cleveland Massillon Road, Norton, OH 44203 USA (the “**Local Education Agency**” or “**LEA**”) and 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, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years unless and until the extent terminated by the parties. Exhibit E will expire 3 years from the date the original DPA was signed unless and until the extent terminated by the parties.
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 Provider for this DPA is:

Name: Jeff Buening Title: District Lead

Address: 2261 Market Street STE 10437

Phone: 513-720-0945 Email: jeff.buening@classdojo.com

The designated representative for the LEA for this DPA is:

Angie Wagler, Coordinator of Technology & Technology Professional Development
awagler@nortonpanthers.org
4128 S Cleveland Massillon Road, Norton, OH 44203 USA
Phone: 330.825.0863 Ext: 532020

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

Norton City Schools

By: *Bryan Farson* Date: Aug 1, 2025
Bryan Farson (Aug 1, 2025 09:58:15 EDT)

Printed Name: Bryan Farson Title/Position: Superintendent

ClassDojo, Inc.

By: *Tina Hwang* Date: Jul 31, 2025

Printed Name: Tina Hwang Title/Position: Head of Legal

ARTICLE I: PURPOSE AND SCOPE

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's Education 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.
3. **Separate Account.** Students and parent users may have personal or non-school accounts (i.e., for use of ClassDojo at home not related to school) in addition to school accounts (“Outside School Account(s)”). An Outside School Account of a student may also be linked to their student account. Student Data shall not include information a student or parent 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, if Student-Generated Content is stored or maintained by the Provider, Provider may, at the request of the LEA, student if the student is over 18, or student's parent or legal guardian if the student is under 18, transfer, or provide a mechanism for the LEA to transfer, said Student- Generated Content to a

separate account created by the student or the Outside School Child Account.

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 except in with a Changes of Control.

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 or other institutions 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; or (c) for any commercial purpose other than to provide (which shall include maintaining, developing, supporting, improving, and diagnosing) the Service to the LEA, or as authorized by the LEA or the parent/guardian. 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 provide recommendations for employment, school, adaptive learning or customized student learning within a school service when such recommendation is not determined in whole or part by payment or other consideration from a third party; 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; (iv) to notify non-Student LEA account holders about new education product updates, features, or services that are not Targeted Advertising; or (v) from otherwise using Student Data as permitted in this DPA and its accompanying exhibits. Furthermore, Provider may not rely on this DPA as the source of verifiable parental consent.

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. 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 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. With respect to the treatment of Student Data, in the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the Supplemental State Terms, the Supplemental State Terms will control. 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

Service Agreement: ClassDojo District Terms of Service are located at <https://www.classdojo.com/district-terms> (entered into by all LEA). The ClassDojo District Terms include additional terms which must be entered into by both LEA and all individual users of the Service, located at <https://www.classdojo.com/terms/> ("ClassDojo Terms of Service"), and which are required to use the services. The ClassDojo District Terms and ClassDojo Terms of Service are collectively the "Service Agreement".

1. **Services:** Pursuant to and as fully described in the Service Agreements, Provider has agreed to provide the Services set forth below. Provider is a school communication and classroom management platform that helps bring teachers, School Leaders, families, and students together. For clarity, if not opting in to use Single Sign On (SSO) or another rostering option ("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. 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 ("Family Communities") where a teacher is not included ("Family Communities"), are not part of the Services
- Classroom Management Tools: Features that allow teachers, [School Leaders](#), and [Admins](#) 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 and School Stories. School 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](#)"): 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 Admins 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. 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 Story, Portfolios, or School Stories). Note, however, that ClassDojo Plus has out-of-school features such as Home Points, At-Home Child Monster with premium parts, and

Discover tab content that the parties agree are not part of the Services (“ClassDojo Plus Non-School Use Features”).

- 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 Terms of Service.
- 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 as 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 [Student Account](#) in the main ClassDojo Services. 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](#).

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 for the education agency, provide products to the education agency, and ensure secure and effective operation of Provider’s products. 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, that could negatively impact the LEA and its authorized users. Provider may also process Student Data for adaptive or personalized learning purposes and to provide Program Communications (as defined in Exhibit C to all account holders).

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

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

2. **Outside School Accounts and Linked Data:**

- (1) The Service shall not include any Outside School Accounts and those products and features set forth in this [Exhibit “A”](#). Additionally, the Service shall not include any online live tutoring services offered for children through the website located at <https://tutor.classdojo.com/> (“**Dojo Tutor**”). The Parties agree that an Outside School Account of a student may also be linked to their student account with the Student Data elements as further described in the “Linked Accounts” section of the Service Agreement (“Linked Data”) and set forth [here](#).
- (2) 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

3. **Provider Use of Account Data**

The Parties agree that Provider shall independently use certain limited Account Data (as defined below) collected in connection with the Services.

“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, for one of the following exhaustive list of purposes:

Billing, account, and LEA and LEA end user relationship management, including for ClassDojo product recommendations and Program Communications and related end user correspondence (e.g., mailings about necessary updates and product capabilities); 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, so long as no Student Data is used;

Any Family Messaging and Family Communities as defined above; and Product development and optimization, so long as no Student Data is used.

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.	<input checked="" type="checkbox"/>
	Other application technology meta data-Please specify: https://www.classdojo.com/cookies-policy https://classdojo.com/transparency	<input checked="" type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input checked="" type="checkbox"/>
	Other assessment data-Please specify: Observation data is 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, and data does not include product events.	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data <i>Optional, only if teacher(s) elect to record</i>	<input checked="" type="checkbox"/>
Communications	Online communications captured (emails, blog entries) <i>Optional</i>	<input checked="" type="checkbox"/>
Conduct	Conduct or behavioral data <i>Optional</i>	<input type="checkbox"/>
Demographics	Date of Birth <i>Age, not Date of Birth</i>	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, or primary language spoken by student) <i>Obtained via browser/device preferences</i>	<input checked="" type="checkbox"/>
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Parent/Guardian ID	<i>Parent ID number is created to link parents to students</i>	<input checked="" type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input checked="" type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input checked="" type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>
	Email <i>Only for students whose teachers elect to utilize the Google Login method.</i>	<input checked="" type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Provider/App assigned student ID number	<input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/>
Student Name	First and/or Last	<input checked="" type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level) <i>We track product events and progress within a particular feature</i>	<input checked="" type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input checked="" type="checkbox"/>
	Other student work data -Please specify: Note Student generated content may also be teacher-assigned projects.	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/ performance scores	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System
Other	<p>Please list each additional data element used, stored, or collected by your application:</p> <p>Please see the Information Transparency Chart (https://www.classdojo.com/transparency) for additional details regarding:</p> <ul style="list-style-type: none"> • 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 <p>Current list of Sub-Processors: https://www.classdojo.com/third-party service-providers/</p>	<input checked="" type="checkbox"/>
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	<input type="checkbox"/>

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

[Insert Name of District or LEA] Provider to dispose of Student Data obtained by Provider pursuant to the terms of the DPA between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[Insert categories of data here]

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

Student-Generated Content will be kept if a user has an Outside School Account and kept in such Outside School Account.

2. Nature of Disposition

☒ Disposition shall be by destruction or deletion of Student Data.

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

[Insert or attach special instructions]

3. Schedule of Disposition

Student Data shall be disposed of by the following date:

☒ As soon as commercially practicable. at the earliest of (a) Provider's standard destruction schedule, if applicable; (b) when the Student Data is no longer needed for the purpose for which it was received; or (c) as otherwise required by law.

☐ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and **Norton City Schools** ("Originating LEA") which is dated Aug 1, 2025 , 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 statutes; (2) a material change in the services and products listed in the originating Service Agreement; or (3) three years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following **email address:**
privacy@classdojo.com.

ClassDojo, Inc.

Tina Hwang

BY: _____ Date: Jul 31, 2025

Printed Name: Tina Hwang Title/Position: Head of Legal

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 **Norton City Schools** and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

BY: _____ Date: _____

Printed Name: _____ Title/Position: _____

SCHOOL DISTRICT NAME: _____

DESIGNATED REPRESENTATIVE OF LEA:

Name: _____

Title: _____

Address: _____

Telephone Number: _____

Email: _____

EXHIBIT “F”
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

Cybersecurity Frameworks

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

More details available at ClassDojo’s Security Overview: <https://www.classdojo.com/security>

EXHIBIT "G"
Massachusetts

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Massachusetts. Specifically, those laws are 603 C.M.R. 23.00, Massachusetts General Law, Chapter 71, Sections 34D to 34H and 603 CMR 28.00; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Massachusetts;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Massachusetts does not require data to be stored within the United States.

EXHIBIT "G"
Maine

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Maine. Specifically, those laws are 20-A M.R.S. §6001-6005.; 20-A M.R.S. §951 et. seq., Maine Unified Special Education Regulations, Maine Dep't of Edu. Rule Ch. 101; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Maine;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Maine does not require data to be stored within the United States.
4. The Provider may not publish on the Internet or provide for publication on the Internet any Student Data.
5. If the Provider collects student social security numbers, the Provider shall notify the LEA of the purpose the social security number will be used and provide an opportunity not to provide a social security number if the parent and/or student elects.
6. The parties agree that the definition of Student Data in Exhibit "C" includes the name of the student's family members, the student's place of birth, the student's mother's maiden name, results of assessments administered by the State, LEA or teacher, including participating information, course transcript information, including, but not limited to, courses taken and completed, course grades and grade point average, credits earned and degree, diploma, credential attainment or other school exit information, attendance and mobility information between and within LEAs within Maine, student's gender, race and ethnicity, educational program participation information required by state or federal law and email.
7. The parties agree that the definition of Student Data in Exhibit "C" includes information that:
 - a. Is created by a student or the student's parent or provided to an employee or agent of the LEA or a Provider in the course of the student's or parent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes;
 - b. Is created or provided by an employee or agent of the LEA, including information provided to the Provider in the course of the employee's or agent's use of the Provider's website, service or application for kindergarten to grade 12 school purposes; or
 - c. Is gathered by the Provider through the operation of the Provider's website, service or application for kindergarten to grade 12 school purposes.

EXHIBIT “G”
Iowa

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Iowa. Specifically, those laws are Iowa Code §§ 22; Iowa Code §§ 715C, 281 I.A.C. 12.3(4); 41; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Iowa;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Iowa does not require all Student Data to be stored within the United States.
4. In Exhibit “C” add to the definition of “Student Data” significant information on progress and growth, experiences, interests, aptitudes, attitudes, abilities, part-time employment, and future plans.

EXHIBIT “G”

Missouri

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Missouri. Specifically, those laws are Sections 162.1475 and 407.1500 RSMo; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Missouri;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Missouri does not require data to be stored within the United States.
4. Replace Article V, Section 4(1) with the following:
 - a. In the event of a breach of data maintained in an electronic form that includes personal information of a student or a student’s family member, Provider shall notify LEA within seventy-two (72) hours. The notice shall include (if and to the extent this information is known to the Provider):
 - i. Details of the incident, including when it occurred and when it was discovered;
 - ii. The type of personal information that was obtained as a result of the breach; and
 - iii. The contact person for Provider who has more information about the incident.
 - b. “*Breach*” shall mean the unauthorized access to or unauthorized acquisition of personal information that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by a person employed by or contracted with, or an agent of, Provider is not a breach provided that the personal information is not used in violation of applicable Federal or Missouri law, or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.
 - c. “*Personal information*” is the first name or initial and last name of a student or a family member of a student in combination with any one or more of the following data items that relate to the student or a family member of the student if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology such that the name or data elements are unreadable or unusable:
 - i. Social Security Number;
 - ii. Driver’s license number or other unique identification number created or collected by a government body;
 - iii. Financial account information, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - iv. Unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual’s financial account;
 - v. Medical information; or
 - vi. Health insurance information.

Nebraska

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Nebraska. Specifically, those laws are Neb. Rev. Stat. Secs. 79-2,104; 79-2,153 to 79-2,155; 79-2, 539; 87-801 to 87-808; and 92 NAC 6; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Nebraska;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article II, Section 5, add, “Specifically, any written agreement with a Subprocessor will: (1) prohibit the Subprocessor from using Student Data any purpose other than providing the contracted service to or on behalf of the Provider; (2) prohibit the Subprocessor from disclosing any Student Data provided by the Provider with subsequent third parties who are not their own subprocessors; (3) and requires the Subprocessor to implement and maintain reasonable security procedures and practices.”
2. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
3. In Article IV, Section 4, replace: “Provider will not Sell Student Data to any third party” with “Provider will not Sell or rent Student Data to any third party.”
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Nebraska does not require data to be stored within the United States.

EXHIBIT "G"
New Jersey

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in New Jersey. Specifically, those laws are N.J. Stat. § 56:8-166.4 et seq.; N.J. Stat. § 18A:36-19; N.J. Stat. § 18A:36-19a; N.J. Stat. § 18A:36-35; N.J. Admin Code § 6A:16-7.9; N.J. Admin. Code § 6A:32-2.1; N.J. Admin. Code § 6A:32-7 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for New Jersey;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. The Provider will not disclose on its web site without the written permission of a parent or guardian any personally identifiable information about a student, including, but not limited to student names, student photos, student addresses, student e-mail addresses, student phone numbers, and locations and times of class trips.
4. The Provider will not process Student Data in violation of applicable State and federal laws that prohibit unlawful discrimination.
5. The Provider will not conduct processing that presents a heightened risk of harm to students without conducting and documenting a data protection assessment of each of its processing activities that involve Student Data.
6. In Article V, Section 1 Data Storage: New Jersey does not require data to be stored within the United States.
7. Add to the definition in Exhibit "C" of Student Data: "The location and times of class trips."

EXHIBIT "G"

Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Ohio. Specifically, those laws are R.C. §§ 3319.32-3319.327, R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. In Article IV, Section 6, replace "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," with "Upon termination of this DPA, unless the LEA provides notice that renewal of the contract is reasonably anticipated, within ninety (90) days of the expiration of the contract, Provider shall destroy or return Student Data to the LEA."
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.
6. Provider will not access or monitor any of the following:
 - a. Location-tracking features of a school-issued device;
 - b. Audio or visual receiving, transmitting or recording features of a school-issued device;
 - c. Student interactions with a school-issued device, including, but not limited to, keystrokes and web-browsing activity

Notwithstanding the above, if the Provider has provided written notice to the LEA that it engages in this collection of the above information, which must be provided in the Service Agreement, and the LEA has provided written confirmation that the Provider can collect this information pursuant to its general monitoring, then the Provider may access or monitor the listed information.

EXHIBIT "G"
Rhode Island

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Rhode Island. Specifically, those laws are R.I.G.L. 16-71-1, et. seq., R.I.G.L. 16- 104-1, and R.I.G.L., 11-49.3 et. seq.; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Rhode Island;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Rhode Island does not require data to be stored within the United States.
4. The Provider agrees that this DPA serves as its written certification of its compliance with R.I.G.L. 16-104-1, as amended as follows: R.I.G.L.16-1904-1: (b) Notwithstanding any general or special law to the contrary, any person who provides a cloud computing service to an educational institution operating within the state shall process data of a student enrolled in kindergarten through twelfth (12th) grade for the sole purpose of providing the cloud computing service to the educational institution and shall not, except with the permission of a parent or guardian, process such data for any commercial purposes, including, but not limited to, advertising purposes that benefit the cloud computing service provider.
5. The Provider agrees to implement and maintain a risk-based information security program that contains reasonable security procedures.
6. In the case of a data breach, as a part of the security breach notification outlined in Article V, Section 4(1), the Provider agrees to provide the following additional information if and to the extent the Provider has knowledge of such information and to the extent Provider is required to do so by applicable law:
 - i. Information about what the Provider has done to protect individuals whose information has been breached, including toll free numbers and websites to contact, if applicable:
 1. The credit reporting agencies
 2. Remediation service providers
 3. The attorney general
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
 - iii. A clear and concise description of the affected parent, legal guardian, staff member, or eligible student's ability to file or obtain a police report; how an affected parent, legal guardian, staff member, or eligible student's requests a security freeze and the

necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

EXHIBIT "G"
Tennessee

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Tennessee. Specifically, those laws are T.C.A. §§ 10-7-503 *et. seq.*, T.C.A. § 47-18-2107, T.C.A. § 49-1-701 *et. seq.*, T.C.A. § 49-2-211, T.C.A. § 49-6-902, § 49-6-3001, T.C.A. §§ 49-50-1501 *et. seq.*; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Tennessee;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Tennessee does not require data to be stored within the United States.
4. The Provider agrees that it will not collect any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.
5. The Provider agrees that it will not collect individual student data on:
 - a. Political affiliation;
 - b. Religion;
 - c. Voting history; and
 - d. Firearms ownership

EXHIBIT "G"

Vermont

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to several state laws in Vermont. Specifically, those laws are 9 VSA 2443 to 2443f; 16 VSA 1321 to 1324; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Vermont;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required" and delete "or stated in the Service Agreement."
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Vermont does not require data to be stored within the United States.

EXHIBIT “G”
Virginia

WHEREAS, the documents and data transferred from LEAs and created by the Provider’s Services are also subject to several state laws in Virginia. Specifically, those laws are Code of Virginia § 22.1-289.01 and Virginia Code § 2.2-5514(c); and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Virginia;

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

1. In Article IV, Section 2, replace “otherwise authorized,” with “otherwise required” and delete “or stated in the Service Agreement.”
2. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
3. In Article V, Section 1 Data Storage: Virginia does not require data to be stored within the United States.
4. In Article V, Section 4, add: In order to ensure the LEA’s ability to comply with its reporting requirements under Virginia Code § 2.2-5514(c), Provider shall provide initial notification to the LEA as soon as reasonably practical, and at a minimum within twenty-four (24) hours, where the Provider reasonably expects or confirms Student Data may have been disclosed in a data breach.

EXHIBIT "I" – TEACHER DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	✓
	Other application technology meta data-Please specify: <i>Server Log information, device specific information (model, device ID), browser type.</i>	✓
Application Use Statistics	Meta data on user interaction with application	✓
Communications	Online communications that are captured (emails, blog entries)	✓
Demographics	Date of Birth	
	Place of Birth	
	Social Security Number	
	Ethnicity or race	
	Other demographic information-Please specify: <i>device language preference</i>	✓
Personal Contact Information	Personal Address	
	Personal Email	
	Personal Phone	
Performance evaluations	Performance Evaluation Information	
Schedule	Teacher scheduled courses <i>Potentially partial if provided via optional SIS integration for rostering.</i>	✓
	Teacher calendar	
Special Information	Medical alerts	
	Teacher disability information	
	Other indicator information-Please specify:	
Teacher Identifiers	Local (School district) ID number	✓
	State ID number	
	Vendor/App assigned student ID number	✓
	Teacher app username	✓
	Teacher app passwords	✓
Teacher In App Performance	Program/application performance	✓
Teacher Survey Responses	Teacher responses to surveys or questionnaires	
Teacher work	Teacher generated content; writing, pictures etc.	✓
	Other teacher work data -Please specify: <i>Feedback Points (optional feature)</i>	✓
Education	Course grades from schooling	
	Other transcript data -Please specify:	
Other	Please list each additional data element used, stored or collected by your application	✓









ClassDojo_NortonOH_Clean - Copy

Final Audit Report

2025-08-01

Created:	2025-07-31
By:	Ramah Hawley (rhawley@tec-coop.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAA4WVvYJmoPDgCeJ4UvLF8H8VsX2G2sobK

"ClassDojo_NortonOH_Clean - Copy" History

-  Document created by Ramah Hawley (rhawley@tec-coop.org)
2025-07-31 - 8:24:07 PM GMT
-  Document emailed to Tina Hwang (tina.hwang@classdojo.com) for signature
2025-07-31 - 8:24:17 PM GMT
-  Email viewed by Tina Hwang (tina.hwang@classdojo.com)
2025-07-31 - 8:27:21 PM GMT
-  Document e-signed by Tina Hwang (tina.hwang@classdojo.com)
Signature Date: 2025-07-31 - 8:59:27 PM GMT - Time Source: server
-  Document emailed to Bryan Farson (bfarson@nortonpanthers.org) for signature
2025-07-31 - 8:59:29 PM GMT
-  Email viewed by Bryan Farson (bfarson@nortonpanthers.org)
2025-08-01 - 1:57:18 PM GMT
-  Document e-signed by Bryan Farson (bfarson@nortonpanthers.org)
Signature Date: 2025-08-01 - 1:58:15 PM GMT - Time Source: server
-  Agreement completed.
2025-08-01 - 1:58:15 PM GMT



Adobe Acrobat Sign