CLASSDOJO STUDENT DATA PRIVACY ADDENDUM

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

RECITALS

WHEREAS, the Provider is providing educational or digital Services (as defined below) to LEA, which Services may include: (a) cloud-based Services for the digital storage, management, and retrieval of education records; and/or (b) digital educational software that authorizes Provider to access, store, and use education records;

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

WHEREAS, the Provider 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 Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. § 1232h; the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), and applicable state privacy laws and regulations; and

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

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

1. **Standard Schedule**. A description of the Service Agreement, and the categories of Student Data that may be processed by the Provider on behalf of LEA, and other information specific to this DPA are attached as **Exhibit "A" ("Standard Schedule")**.

2. **Services**. The digital educational services and any other products and services that Provider may provide now or in the future to LEA pursuant to the Agreement (the "**Services**") are set forth in the Standard Schedule.

3. **Standard Clauses**. The Student Data Protection Clauses ("Standard Clauses")[1] attached hereto as **Exhibit "B"** are hereby incorporated by reference into this DPA in their entirety.

4. **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.

5. **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.

6. **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, 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

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

Privacy Policy, the terms of this DPA shall apply and take precedence. 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.

7. **Notices**. All notices or other communication required or permitted to be given hereunder must be made in writing and may be given via e-mail transmission, or first-class mail, or mutually agreed upon method sent to the designated representatives set forth in the Standard Schedule.

8. **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. For clarity, nothing in this Section prohibits Provider from amending the Service Agreement pursuant to the amendment provisions set forth therein.

9. **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.

10. **Governing Law; Venue and Jurisdiction**. This DPA will be governed by and construed in accordance with the laws of the state of the LEA signing the DPA, without regard to conflicts of law principles. Each Party consents and submits to the sole and exclusive jurisdiction to the state and federal courts for the county of the LEA for any dispute arising out of or relating to this DPA or the transactions contemplated hereby.

11. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a Change of Control (as defined in Exhibit C). In the event of a Change of Control, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of such Change of Control. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement.

12. **Waiver**. No delay or omission by either party to exercise any right, power or privilege hereunder shall be construed as a waiver of any such right, nor shall any single or partial exercise of any such right, power or privilege preclude any further exercise thereof, and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

13. **Electronic Signature**: The Parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with applicable state and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of their electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

Signatory Information

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

Name of LEA or District: _____

Address: _____
Street Address

_____
Address Line 2

_____
City, State / Province / Region

_____
Postal / Zip Code, Country

LEA Authorized Representative Name: _____

Title, Role, or Position: _____

Email: _____

LEA Authorized Representative's Signature: _____

ClassDojo Representative Signature: 

ClassDojo Representative Full Name: Jeff Buening

Title, Role, or Position: District Partnerships, General Manager

Email: jeff.buening@classdojo.com; districts@classdojo.com

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

Date: January 1, 2025

EXHIBIT "A"

STANDARD SCHEDULE

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

2. **Services**: Pursuant to and as fully described in the Service Agreements, Provider has agreed to provide the Services set forth below. Provider is a school communication and classroom management platform that helps bring teachers, School Leaders, families, and students together. For clarity, if not opting in to use Single Sign On (SSO) or another rostering option ("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 ("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, 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 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 users or others, or the security of the Services. ClassDojo may also use De-Identified Data for (i) product improvement and new educational product development; (ii) sharing reports on number of users, instructional time delivered or other reports on product usage and results to third parties; (iii) educational research purposes, including transferring or sharing with third parties for such purposes; and (iv) as allowed by laws.

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

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

   (1) The Service shall not include any Outside School Accounts and those products and features set forth in 3(b) of 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

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:

   (1) 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);

   (2) 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;

(3) Any Family Messaging and Family Communities as defined above; and

(4) Product development and optimization.

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

Notices to Provider

ClassDojo, Inc.
2261 Market Street STE 10437
San Francisco, CA 94114

districts@classdojo.com, with a copy to
legalprocess@classdojo.com

Notice to LEA
LEA Name: _____

LEA E-Mail Address: _____

LEA Mailing Address: _____

With a copy to LEA Legal Counsel (if provided)
LEA Legal Counsel Address: _____

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

Name: _____

Title: _____

E-Mail Address: _____

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

Name: _____

Title: _____

E-Mail Address: _____

Provider Contact:
Jeff Buening, District Partnerships, districts@classdojo.com

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

Schedule of Student Data**

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

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	✓ https://www.classdojo.com/cookies-policy
	Other application technology metadata.	✓ https://www.classdojo.com/transparency
Application Use Statistics	Metadata on user interaction with application	✓ We track product events and progress within a particular feature
Assessment	Standardized test scores	N/A
	Observation data	✓ Optional, only if teacher(s) opt to use the "Feedback Points" feature is this collected from teachers about students. *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 "B"
STANDARD CLAUSES
January 2025

Article I: PURPOSE AND SCOPE

1.1. Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data, including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. 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. With respect to its use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA as set forth in this DPA and the Service Agreement.

1.2. 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.

1.3. Student Data to Be Provided.
In order to perform the Services, the Provider shall process Student Data as identified by the Provider in the Schedule of Data, attached hereto to the Standard Schedule. 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.

1.4. DPA Definitions. The definition of terms used in this DPA shall have the meaning set forth in **Exhibit "C".** With respect to the treatment of Student Data, in the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

2.1 Student Data Property of LEA. As between LEA and Provider, all Student Data processed by the Provider (as set forth fully in the definition of Student Data) pursuant to the Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data processed by the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA or the party who provided such data (such as the student or parent).

2.2 Parent, Legal Guardian, and Student Access. The LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student (as defined in FERPA) may review Student Data and request deletion or modification, and request delivery of a copy of the Student Data. In support of this, the Provider shall establish reasonable procedures by which the LEA may access, and correct if necessary, Education Records and/or Student Data, and make a copy of the data available to the LEA (or at the LEA's direction) to the parent, legal guardian or eligible student directly. If the LEA is not able to review or update the Student Data itself, Provider shall respond in a reasonably timely manner (and no later than thirty (30) 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, legal guardian, or student, whichever is sooner) to the LEA's request for Student Data held by the Provider to view or correct as necessary.

In the event that a parent or legal guardian of a student or an eligible student contacts the Provider to correct, delete, review, or request delivery of a copy of any of the Student Data collected by or generated through the Services, the Provider shall refer that person 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. In the event that any person other than those listed contacts the Provider about any Student Data, the Provider shall refer that person to the LEA, except as provided in Article IV, Section 4.4.

2.2.1 This DPA does not impede the ability of students, or the 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.

2.2.2 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.

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; provided, however, such transfer shall only apply to Student Generated Content that is severable from the Service.

2.4 Subprocessors. Provider shall enter into a Subprocessor 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).

ARTICLE III: DUTIES OF LEA

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

3.2 Annual Notification of Rights. If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a School Official and what constitutes a legitimate educational interest in its annual notification of FERPA rights ("**Annual Notification of Rights**"). Additionally, LEA represents, warrants and covenants to Provider, as applicable, that LEA has:

a. Complied with the School Official Exemption, including, without limitation, informing parents in their Annual Notification of Rights that the LEA defines School Official to include 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.

3.3 Reasonable Precautions. LEA shall employ administrative, physical and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted Student Data from unauthorized access, disclosure or acquisition by an unauthorized person.

3.4 Unauthorized Access Notification and Assistance. LEA shall notify Provider within seventy-two (72) hours, of any 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 provide reasonable assistance to Provider in any efforts by Provider to investigate and respond to such Data Breach.

ARTICLE IV: DUTIES OF PROVIDER

4.1 Privacy and Security Compliance. The Provider shall comply with all laws, and regulations applicable to Provider's protection of Student Data privacy and security in connection with the Provider providing the Service to the LEA.

4.2 Authorized Use. The Student Data processed pursuant to the Agreement, shall be used by the Provider for no purpose other than performing the Services outlined in **Exhibit "A",** as stated in the Service Agreement, as instructed by the LEA, and/or otherwise authorized under law.

4.3 Provider Employee Obligation. Provider shall require all of Provider's employees 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 with access to Student Data pursuant to the Service Agreement.

4.4 No Disclosure. Provider acknowledges and agrees that it shall not Sell or disclose 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.

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.

4.5 De-Identified Data. Provider agrees not to attempt to re-identify De-Identified Student Data without the written direction of the LEA. De-Identified Student 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, as well as the following purposes (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) research development and improvement of the Provider's educational sites, Services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Student Data shall survive termination of this DPA or any request by LEA to return or dispose of Student Data. Provider agrees not to transfer De-Identified Student Data to any third party unless that party agrees in writing not to attempt re-identification. Prior to publicly publishing any document that names the LEA, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Student Data is presented. 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.

4.6 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.

At the termination of this DPA, Provider shall, unless directed otherwise by the LEA, dispose of, or delete, Student Data obtained by the Provider under the 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. The LEA may provide the Provider with special instructions for the disposition of the Student Data, by transmitting to Provider **Exhibit "D"**, attached hereto. The duty of the Provider to dispose of or delete Student Data shall not extend to De-Identified Data; Student-Generated Content that has been transferred or kept pursuant to Section 2.2.2.; or Linked Data.

4.7 Advertising Limits. Provider is prohibited from using, disclosing, or Selling Student Data to (a) inform, influence, or enable Targeted Advertising; (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA, or as authorized by the parent or legal guardian; or (c) for any commercial purpose other than to provide (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. Targeted Advertising is strictly prohibited. However, this section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations or sending Program Communications to account holders); or (ii) to provide 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; 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; or (v) from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA SECURITY AND BREACH PROVISIONS

5.1 Data Storage. If Student Data is stored outside the United States, Provider will provide a list of the countries where Student Data is stored through its disclosure set forth here: https://www.classdojo.com/third-party-service-providers/

5.2 Security Audits. No more than once per contract year, or following a Security Incident, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit, during normal business hours and at a time convenient for the Provider, the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of Services to the LEA ("**Security Audit**"). In connection with any Security Audit, the Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA, as reasonably necessary to fulfill the requests of such Security Audit. Costs for the Security Audit are the responsibility of the LEA. 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.

5.3 Data Security. The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security of Student Data. The Provider shall implement an adequate Cybersecurity Framework that incorporates one or more of the nationally or

internationally recognized standards set forth in **Exhibit "E"**. Additionally, Provider may choose to further detail its security programs and measures in **Exhibit "E"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

5.4 Data Breach. In the event that Provider confirms a Data Breach, the Provider shall provide notification to LEA as required by the applicable state law, but in no event later than seventy-two (72) hours of confirmation of the Data Breach ("**Data Breach Notification**"), unless notification within this time limit would disrupt investigation of the Data Breach, by either the Provider or by law enforcement. In such an event, the Data Breach Notification shall be made within a reasonable time after the discovery of the 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, the Data Breach Notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
   (a) The name and contact information of the Provider subject to this section,
   (b) The date of the Data Breach Notification,
   (c) The date of the Data Breach, the estimated date of the Data Breach or the date range within which the Data Breach occurred,
   (d) Whether the notification was delayed as a result of a law enforcement investigation, if legally permissible to share that that information,
   (e) A general description of the Data Breach, if that information is possible to determine at the time the Data Breach Notification is provided,
   (f) A description of the Student Data reasonably believed to have been the subject of the Data Breach; and
   (g) Identification of impacted individuals

(2) Provider agrees to adhere to all requirements applicable to Provider providing the Services in applicable federal and state law with respect to a Data Breach related to the Student Data, including, any 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 is consistent with applicable industry standards and federal and state law for responding to a Data Breach involving Student Data ("**Incident Response Plan**") and agrees to provide LEA, upon reasonable written 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.

(5) In the event of a Data 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.

ARTICLE VI: INTERNATIONAL DATA PROTECTION ADDENDUM

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

EXHIBIT "C": DEFINITIONS

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.

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 Records: Education 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.

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.

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.

"Sell". For the purposes of this DPA, "Sell", or "Selling" does not include those actions described as permitted in Article IV, Section 4.4.1 In addition, Provider is also not "selling" personal information (i) if a user directs Provider to intentionally disclose Student Data or uses the Service to intentionally interact with a third party, provided that such third party also does not Sell the Student Data; or (ii) if a parent or other third party authorized by the parent lawfully acquires Student Data (e.g., enhanced classroom reports or photos) for a fee or for free.

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

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, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, for a school purpose, that is descriptive of the student including, but not limited to, information in the student's Education Record, persistent unique identifier, or any other information or identification number that would provide information about a specific student. Student Data includes Metadata that has not been stripped of all direct and indirect identifiers. Student Data further includes Personally Identifiable Information, 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 "A"** (Standard Schedule) within the Schedule of Data is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not include Student-Generated Content or De-Identified Data or information that has been anonymized, or anonymous usage data regarding a student's or LEA's use of Provider's Services. Student Data shall 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

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

Subprocessor Agreement: An agreement between the Provider and a third party Subprocessor. A Subprocessor Agreement includes either a written agreement or an acceptance of terms and conditions (e.g. click through agreements).

Targeted Advertising: 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 Provider's Internet website, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include Contextual Advertising, or in response to a student's response or request for information or feedback.

EXHIBIT "D":

SPECIAL INSTRUCTIONS FOR DISPOSITION OF STUDENT DATA

After this DPA takes effect, if the LEA has special requirements for the disposition of Student Data, that are not expressed in Article IV, Section 4.6 "Disposition of Data", the LEA may fill in this form and deliver it to the Provider.

The Provider and the LEA must not fill in this form at the initiation of the DPA. The Provider shall act on "Exhibit D" from the designated representative of the LEA or their designee (set forth in the Standard Schedule)

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

1. **Extent of Disposition**

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

[Insert categories of Student Data here]

☐ Disposition is complete. Disposition extends to all categories of Student Data.

2. **Nature of Disposition**

☐ Disposition shall be by destruction or deletion of Student Data, as set forth in Section 4.6 ("Disposition of Data").

☐ Disposition shall be by a transfer of Student Data. The Student Data shall be transferred to the following site as follows:
[Insert or attach special instructions]

3. **Timing of Disposition**

Student Data shall be disposed of by the following date:

☐ As soon as commercially practicable

☐ On Provider's standard destruction schedule

☐ By *[Insert Date]*

4. **De-Identified Data**

[ ] The Provider certifies that they have De-Identified the Student Data, as defined elsewhere in this Agreement, and disposed of all copies of Student Data that were not De-Identified in accordance with this Schedule and the DPA. The Provider will notify LEA in accordance with the notification requirements of the DPA using this form.

As of *[Insert Date]*

5. **Other:**

Signature(s) **Notice of Verified Disposition of Data**

Authorized Representative of LEA Date

Authorized Representative of Company Date

EXHIBIT "E":

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

Provider must mark one or more frameworks with which it complies.

The Provider may change which framework it complies with without invalidating or changing the DPA, but must notify the LEA of such change in accordance with the notification requirements of the DPA.

	FRAMEWORK(S)
✓	**NIST Cybersecurity Framework (CSF)**
	NIST SP 800-53 Security and Privacy Controls for Information systems and organizations
	NIST SP 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
	ISO 27000 series, Standards for implementing organization security and management practices
	CIS Center for Internet Security Critical Security Controls
	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

ClassDojo Specific: Please review ClassDojo's Security Overview for additional details: https://www.classdojo.com/security/