NEW HAMPSHIRE STUDENT DATA PRIVACY AGREEMENT VERSION (2019)

Franklin School District

and

ClassDojo, Inc.

July 31, 2020

This New Hampshire Student Data Privacy Agreement ("DPA") is incorporated by reference into the Service Agreement (as defined below) entered into by and between the school district, Franklin School District (hereinafter referred to as "LEA") and ClassDojo Inc. (hereinafter referred to as "Provider") on July 31, 2020. (each of Provider and LEA, a "Party" and together "Parties"). The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the LEA with certain digital educational services as described in Article I and Exhibit "A"; pursuant to the ClassDojo Terms of Service located at https://www.classdojo.com/terms (the "Service Agreement"); and

WHEREAS, the Provider, by signing this Agreement, agrees to allow the LEA to offer school districts in New Hampshire the opportunity to accept and enjoy the benefits of the DPA for the Services (as defined below) described, without the need to negotiate terms in a separate DPA; and

WHEREAS, in order to provide the Services described in Article 1 and Appendix A, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA"), 20 U.S.C. §§ 1400 et. seq., 34 C.F.R. Part 300; and

WHEREAS, the documents and data transferred from New Hampshire LEAs and created by the Provider's Services are also subject to several New Hampshire student privacy laws, including RSA 189:1-e and 189:65-69; RSA 186; NH Admin. Code Ed. 300 and NH Admin. Code Ed. 1100; and

WHEREAS, the Parties wish to enter into this 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.

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

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 (as defined in Exhibit "C") transmitted to Provider from the LEA and it's users pursuant to the Service Agreement including compliance with all applicable federal and state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100; and other applicable New Hampshire state laws, all as may be amended from time to time. This DPA, together with the Service Agreement is the "Agreement".

2. **Nature of Services Provided**. Pursuant to and as fully described in the Service Agreement, Provider has agreed to provide the following digital educational services described in Exhibit "A". hereto and any other products and services that Provider may provide now or in the future (the "Services").

3. **Student Data to Be Provided**. In order to perform the Services described in this Article and the Service Agreement, LEA and Provider shall indicate the categories of data described in the Schedule of Data, attached hereto as Exhibit "B".

4. **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 all other writings, including, but not limited to, the Service Agreement, privacy policies or any terms of service with respect to the treatment of Student Data.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data or any other Education Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA, or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Education Records transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are also subject to the provisions of this Agreement in the same manner as the original Student Data or Education Records. The Parties agree that as between them, all rights, including all intellectual property rights, in and to Student Data or any other Education Records contemplated per this Agreement shall remain the exclusive property of the LEA, or the party who provided such data (such as the student or parent). The Parties agree that the LEA will be able to access and transfer Student Data to a separate account as necessary.
2. **Exemptions under FERPA.** LEA may not generally disclose Personally Identifiable Information from an eligible student's Education Records to a third-party without written consent of the parent and/or eligible student or without meeting one of the exemptions set forth in FERPA ("FERPA Exemption(s)"), including the School Official exemption ("School Official Exemption"). For the purposes of FERPA, to the extent Personally Identifiable Information from Education Records are transmitted to Provider from LEA or from students using accounts at the direction of the LEA, the Provider shall be considered a School Official (as defined on Exhibit C), under the control and direction of the LEAs as it pertains to the use of Education Records. Control duties are set forth below.

3. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Personally Identifiable Information contained in the related student's Education Records and correct erroneous information, and procedures for the transfer of Pupil-Generated Content to a personal account, consistent with the functionality of Services. Provider shall cooperate and respond within ten (10) days to the LEA's request for Personally Identifiable Information contained in the related student's Education Records held by the Provider to view or correct as necessary. In the event that a parent/legal guardian of a student or other individual contacts the Provider to review any of the Education Records or 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.

4. **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 and such information will be kept separate from the Student Data subject to this DPA. Additionally, if Pupil-

Generated Content is stored or maintained by the Provider as part of the Services, Provider may, at the request of the LEA or parent or legal guardian, transfer Pupil- Generated Content to a separate student account or the Outside School Account upon termination of the Agreement.

5. **Third Party Request**. Should a Third Party, excluding a Subprocessor, including, but not limited to law enforcement, former employees of the LEA, current employees of the LEA, and government entities, contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA, unless and to the extent that Provider reasonably believes it must grant such access to the third party because the data disclosure is necessary: (i) pursuant to a court order or legal process, (ii) to comply with statutes or regulations, (iii) to enforce the Agreement, or (iv) in connection with the LEA or its users (including parents, teachers and students), in a health and safety emergency if the LEA determines that the knowledge of the information is necessary to protect the health or safety of the student or other individuals. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited.
6. **No Unauthorized Use**. Provider shall not use Personally Identifiable Information contained in Student Data or in an Education Record for any purpose other than as explicitly specified in this Agreement.
7. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA. 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

1. **Provide Data In Compliance With Laws**. LEA shall provide Student Data for the purposes of the Agreement in compliance with any applicable state or federal laws and regulations pertaining to data privacy and security, including, without limitation, the FERPA, PPRA, IDEA, RSA 189:1-e and 189:65 through 69; RSA 186-C; NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and the other privacy statutes quoted in this DPA. If LEA is providing any Student Data or Education Records to Provider, LEA represents, warrants and covenants to Provider, as applicable, that LEA has:

i. complied with the School Official Exemption, including, without limitation, informing parents in their annual notification of FERPA rights that the Institution defines "school official" to include service providers and defines "legitimate educational interest" to include services such as the type provided by Provider; or

ii. 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.

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.

2. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the Services and/or hosted data.

3. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized use or access of the Services, LEA's account, or Student Data. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized use or access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable New Hampshire and Federal laws and regulations pertaining to data privacy and security, applicable to the Provider providing the Service to LEA. With respect to Student Data that LEA permits Provider to collect or access pursuant to the Agreement, Provider will ensure that its Services help LEA in complying with LEA's obligations under FERPA, PPRA IDEA, RSA 189:1-e, RSA 189:65 through 68 and RSA 186-C, NH Admin. Code Ed. 300; NH Admin. Code Ed. 1100 and all other applicable New Hampshire privacy statutes and regulations.
2. **Authorized Use**. Student Data shared pursuant to this Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services and for the uses set forth in the Agreement and/or as otherwise legally permissible , including, without limitation, for adaptive learning or customized student learning for students from the LEA to provide Services to the students of LEA. The foregoing limitation does not apply to any De-Identified Data (as defined in Exhibit "C").
3. **Employee Obligation.** Provider shall require all 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 this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the DPA.
4. **No Disclosure**. Provider shall not disclose, transfer, Sell, share, lease, trade or rent any Student Data obtained under the Agreement to any other entity other than LEA, except: (i)as authorized by the Agreement; (ii) as directed by LEA; (iii) to authorized (by the LEA or parent) users of the Services, including parents or legal guardians; (iv) as required by law; (v) in response to a judicial order as set forth in Article II, Section 5; (vi) if the LEA determines it is necessary to protect the health or safety of the student or other individuals or the security of the Services; or (vii) to Subprocessors, in connection with operating or improving the Service. Provider will not Sell Student Data.
5. **De-Identified Data**. De-Identified Data may be used by the Provider for any lawful purpose, including, but not limited to, development, research, and improvement of educational sites, services, or applications, and to demonstrate the market effectiveness of the Services. Provider's use of such De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Provider agrees not to attempt to re-identify De-identified Student Data and 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; provided, however, that (b) shall not apply to the transfer to any Subprocessors. 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**. Provider shall, at LEA's request, delete all Personally Identifiable Information contained in Student Data obtained under the DPA upon termination within thirty (30) days for the data and within sixty-five (65) day for any back-ups, according to a schedule and procedure as the Parties may

reasonably agree. If no written request is received, Provider shall dispose of or delete all Personally Identifiable Information contained in Student Data at the earliest of (a) when it is no longer needed for the purpose for which it was obtained or (b) as required by applicable law. Nothing in the DPA authorizes Provider to maintain Personally Identifiable Information contained in Student Data obtained under any other writing beyond the time period reasonably needed to complete the disposition, unless a student, parent or legal guardian of a student chooses to establish and maintain a separate account with Provider for the purpose of storing Pupil- Generated Content. Disposition shall include (1) the shredding of any hard copies of any Personally Identifiable Information contained in Student Data; (2) erasing any Personally Identifiable Information contained in Student Data; or (3) otherwise modifying the Personally Identifiable Information in Student Data to make it unreadable or indecipherable or De-Identified. Provider shall provide written notification to LEA when the Student Data has been disposed pursuant to LEA's request for deletion. The duty to dispose of Student Data shall not extend to Student Data that has been De-Identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" FORM, A Copy of which is attached hereto as Exhibit "D".

7. **Advertising Prohibition**. Provider is prohibited from using Student Data to (a) serve Targeted Advertising to students or families/guardians unless with the consent of parent/guardian or LEA; (b) inform, influence, or enable Targeted Advertising by a Provider unless with the consent of parent/guardian or LEA; (c) develop a profile of a student for any commercial purpose other than providing the Service to LEA or as authorized by the parent/guardian or LEA; or (c) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA and users, as authorized by the parent or legal guardian, or as required by applicable law. This section shall not be construed to limit the ability of Provider to use Student Data for adaptive learning or customized student learning purposes with the LEA's students, including for sending Program Communications to all account holders.

ARTICLE V: SECURITY AND DATA BREACH PROVISIONS

1. **Data Security**. The Provider agrees to employ administrative, physical, and technical safeguards consistent with industry standards designed to protect Student Data from unauthorized access, disclosure, use or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access**. Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees, contractors or Subprocessors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Data shall pass criminal background checks in compliance with state and local ordinances.

    b. **Destruction of Data**. Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the Agreement as set forth in Article 4, Section 6.

c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any Student Data, including ensuring that Student Data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all Student Data obtained or generated pursuant to the Agreement in a secure computer environment and not copy, reproduce, or transmit Student Data obtained pursuant to the Agreement except as necessary to fulfill the purpose of data requests by LEA or as otherwise set forth in the Agreement. The foregoing does not limit the ability of the Provider to allow any necessary Subprocessors to view or access data as set forth in Article IV, section 4.

d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the Services.

e. **Security Technology**. When the Service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect data Student Data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host Student Data pursuant to the Agreement in an environment using a firewall that is periodically updated according to industry standards.

f. **Security Coordinator**. Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the DPA.

g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

h. **Periodic Risk Assessment**. Provider further acknowledges and agrees to conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

i. **Backups.** Provider agrees to maintain backup copies, backed up at least daily, of Student Data in case of Provider's system failure or any other unforeseen event resulting in loss of Student Data or any portion thereof.

j. **Audits.** Upon receipt of a written request from the LEA with at least ten (10) business day notice, the Provider will allow the LEA to audit, during normal business hours and at a time convenient for Provider, the security and privacy measures that are in place to ensure protection of the Student Data or any portion thereof ("Security Audit"). LEA may not request more than more Security Audit per year, except in the case of a verified breach. Notwithstanding the forgoing, the parties agree that the LEA and any local, state, or federal agency with oversight authority/jurisdiction may conduct an audit at any time, in the event an audit is required by governmental or regulatory authorities ("Regulatory Audits"). In connection with any Regulatory Audit or Security Audit, of the Provider , Provider will 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 needed to fulfill the requests of such Regulatory or Security Audit. Failure to cooperate in good faith shall be deemed a material breach of the Agreement. Costs for the audit are the responsibility of the LEA.

k. New Hampshire Specific Data Security Requirements. The Provider agrees to the following privacy and security standards from "the Minimum Standards for Privacy and Security of Student and Employee Data" from the New Hampshire Department of Education. Specifically, the Provider agrees to:

(1) Limit system access to the types of transactions and functions that authorized users, such as students, parents, and LEA are permitted to execute;

(2) Limit unsuccessful logon attempts;

(3) Employ cryptographic mechanisms to protect the confidentiality of remote access sessions;

(4) Authorize wireless access prior to allowing such connections;

(5) Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

(6) Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

(7) Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles;

(8) Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services;

(9) Enforce a minimum password complexity and change of characters when new passwords are created;

(10) Perform maintenance on organizational systems;

(11) Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance;

(12) Ensure equipment removed for off-site maintenance is sanitized of any Student Data in accordance with NIST SP 800-88 Revision 1;

(13) Protect (i.e., physically control and securely store) system media containing Student Data, both paper and digital;

(14) Sanitize or destroy system media containing Student Data in accordance with NIST SP 800-88 Revision 1 before disposal or release for reuse;

(15) Control access to media containing Student Data and maintain accountability for media during transport outside of controlled areas;

(16) Periodically assess the security controls in organizational systems to determine if the controls are effective in their application and develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems;

(17) Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems;

(18) Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception);

(19) Protect the confidentiality of Student Data at rest;

(20) Identify, report, and correct system flaws in a timely manner;

(21) Provide protection from malicious code (i.e. Antivirus and Antimalware) at designated locations within organizational systems;

(22) Monitor system security alerts and advisories and take action in response; and

(23) Update malicious code protection mechanisms when new releases are available.

2. **Data Breach**. In the event that Provider becomes aware of any actual or reasonably suspected unauthorized disclosure of or access to Student Data (a "Security Incident") , Provider shall provide notification to LEA within thirty (30) days of the incident (each a "Security Incident Notification") Provider shall follow the following process:

   a. Unless otherwise required by the applicable law, the Security Incident Notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "When it Occurred," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

   b. The Security Incident Notification described above in section 2(a) shall include such information required by the applicable state law, and at a minimum, the following information:

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

      ii. A list of the types of Personal Identifiable Information that were or are reasonably believed to have been the subject of the Security Incident.

         i. If the information is possible to determine at the time the notice is provided, then either (1) the date of the Security Incident, (2) the estimated date of the Security Incident, or (3) the date range within which the Security Incident

occurred. The Security Incident Notification shall also include the date of the notice.

iii. Whether, to the knowledge of the Provider at the time of the Security Incident was provided, the notification was delayed as a result of a law enforcement investigation. A general description of the Security Incident, if that information is possible to determine at the time the notice is provided.

iv. The estimated number of students and teachers affected by the breach, if any.

c. At LEA's discretion, the Security Incident Notification may also include any of the following:

i. Information about what the Provider has done to protect individuals whose Personally Identifiable Information has been affected by the Security Incident.

ii. Advice on steps that the person whose Personally Identifiable Information has been breached may take to protect himself or herself.

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

e. 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 Security Incident of Student Data or any portion thereof, including Personally Identifiable Information ("Incident Response Plan") and agrees to provide LEA, upon request, with a copy of the Incident Response Plan or a summary of such Incident Response Plan to the extent such Incident Response Plan includes sensitive or confidential information of Provider.

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

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or as required by law.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by terminating the Service Agreement as set forth therein. The LEA or Provider may terminate this DPA and the Service Agreement in the event of a material breach of the terms of this DPA.

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall destroy all of LEA's Personally Identifiable Information contained in Student Data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of Student Data. With respect to the treatment of Student Data, in the event there is conflict between the terms of the DPA, the Service Agreement, or any other agreement between Provider and LEA, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement, or any other agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the designated representatives below.:

   The designated representative for the Provider for this DPA is:

   Elisette Weiss, Privacy Operations, ClassDojo

   [Name/Title]

   Email: elisette@classdojo.com

The designated representative for the LEA for this Agreement is:

Pam McLeod, CETL
Director of Technology | Franklin School District
38 Liberty Street, Franklin, NH 03301
(603) 225.0811 | pmcleod@sau8.org

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

7. **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.

8. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED

IN ACCORDANCE WITH THE LAWS OF THE STATE OF NEW HAMPSHIRE, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS OF MERRIMACK COUNTY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

9. **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 anticipates selling, merging or otherwise disposing of its business to a successor during the term of the Agreement, the Provider shall provide written notice of the proposed sale, merger or disposal to the LEA no later than sixty (60) days prior to the anticipated 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 Agreement if it disapproves of the successor to whom the Provider is selling, merging or otherwise disposing of its business.

10. **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, or employees who may have access to the Student Data and/or any portion thereof.

11. **Waiver**. No delay or omission of the LEA or Provider to exercise any right hereunder shall be construed as a waiver of any such right and the LEA or Provider (as applicable) reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

12. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

ARTICLE VII- 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 this DPA to any other school district in New Hampshire who signs the acceptance in said Exhibit.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this New Hampshire Student Data Privacy Agreement as of the last day noted below.

FRANKLIN SCHOOL DISTRICT

By: Robyn Dunlap Date: 08/14/2020

Printed Name: Robyn Dunlap Title/Position: IT Director

CLASSDOJO INC.

By: Elisette Weiss Date: August 11, 2020

Printed Name: Elisette Weiss Title/Position: District Partnerships & Privacy Operations

EXHIBIT "A"

DESCRIPTION OF SERVICES

ClassDojo is a school communication platform that helps bring teachers, school leaders, families, and students together.

ClassDojo provides the following through its platform:

- A way for teachers to give feedback to students, and other classroom management tools
- Communication tools to help teachers and parents connect with each other
- A way for teachers to share photos, videos, files, and more from the classroom for parents to see
- Student portfolios, where students can share their work with teachers and parents
- Activities and other content that teachers or parents can share with students
- A way for school leaders to see how connected their school community is, and also to communicate with parents

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

EXHIBIT "B"

SCHEDULE OF DATA**

Category of Data	Elements	Check if used by your system
Application Technology Metadata	IP Addresses of users, Use of cookies etc.	✔
	Other metadata; see here: https://www.classdojo.com/transparency	✔
Application Use Statistics	Metadata on user interaction with application	✔
Assessment	Standardized test scores	N/A
	Observation data	✔
	Other assessment data-Please specify:	N/A
Attendance	Student school (daily) attendance data	N/A
	Student class attendance data	✔ if teachers elect to record
Communications	Online communications that are captured (emails, blog entries)	✔ From students if they message directly with their teacher in Portfolios or Class Stories
Biometric Data	Physical or behavioral human characteristics to 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 - we are not passed the information
Conduct	Conduct or behavioral data *For ClassDojo: "Feedback points" are added by the student's teacher*	✔
Demographics	Date of Birth *For ClassDojo: This is collected as an age, not DOB*	✔
	Place of Birth	N/A
	Gender *For ClassDojo: We ask adults for an optional Mr./Miss/etc. salutation*	✔ not from students
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student) *For ClassDojo: This is obtained via browser/device preferences*	✔
	Other demographic information	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	✔
	Phone	✔
Parent/Guardian ID	Parent ID number (created to link parents to students)	✔
Parent/Guardian Name	First and/or Last	✔
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

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	N/A
	Teacher names	✔
Special Indicator	English language learner information	N/A
	Low income status	N/A
	Medical alerts	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 Google Login
	Phone	N/A
Student Identifiers	Local (School district) ID number	✔
	State ID number	N/A
	Vendor/App assigned student ID number	✔
	Student app username	✔
	Student app passwords	✔
Student Name	First and/or Last *For ClassDojo: option to only share last initial*	✔
Student In App Performance	Program/application performance (e.g., typing/reading program performance)	✔ We track product events and progress within a particular function for internal product usage analysis
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. *For ClassDojo: this may also be teacher assigned projects*	✔
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	**

**** Please see the Information Transparency Chart located at: https://www.classdojo.com/transparency for additional details:**

1) Categories of Student Data
2) Categories of Data Subjects the Student Data is collected from and the source of the Student Data
3) Nature and purpose of the Processing activities of the Student Data
4) Country in which the Student Data is stored
5) List of any Special Categories of Student Data collected (currently none)

The current list of Service Providers is located at: https://www.classdojo.com/third-

EXHIBIT "C"

DEFINITIONS

De-Identifiable Information (DII) or De-Identified Data: Means information that has all Personally Identifiable Information ("PII"), including direct and Indirect Identifiers removed or obscured, such that the remaining information does not identify the individual and information about them. The Provider's specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

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

Indirect Identifiers: 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

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" means data, including Indirect Identifiers, that can be used to identify or contact a particular individual, or other data which can be reasonably linked to that data or to that individual's specific computer or device. Student PII includes, without limitation, those items set forth in the definition of PII under FERPA and in the definition under RSA 189:65 and the definition of covered information under RSA 189:68-a. When anonymous or non-personal information is directly or indirectly linked with Personally Identifiable Information, the linked non-personal information is also treated as personal information. Persistent identifiers that are not anonymized, De-Identified or aggregated are personal information. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Program Communications: The term "Program Communications" means 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 and suggestions for additional learning activities in the Service.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education 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 pupil content.

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 education records; and (3) Is subject to FERPA (34 CFR 99.33(a)) governing the use and re-disclosure of personally identifiable information from student records.

Sell: Sell, consistent with the Student Privacy Pledge and R.S.A 189:68-a (II)(a)(3), does not include or apply to a purchase, merger or other type of acquisition of a company by another entity, provided that the company or successor entity continues to treat the Personally Identifiable Information contained in Student Data in a manner consistent with this DPA with respect to the previously acquired Personally Identifiable Information contained in Student Data. Sell also does not include sharing, transferring or disclosing Student Data with a Subprocessor that is necessary to perform a business purpose (such as detecting security incidents, debugging and repairing, storage or other processing activities) provided that the Subprocessor does not further Sell the Student Data except as necessary to perform the business purpose.

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, that is descriptive of the student including, but not limited to, information in the student's Educational Record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number student identifies, search activity, photos, voice recordings or geolocation information. Student Data may include Education Records for the purposes of this Agreement, and for the purposes of New Hampshire and Federal 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 include De-Identified Data or information that has been anonymized, or anonymous usage data regarding a student's use of Provider's Services.

Subscribing LEA: An LEA that was not party to the original DPA and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, 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 software, and who has access to PII.

Targeted Advertising means presenting an advertisement or marketing to a student on the Provider's site, service, or application, or on any other site, service, or application where the selection of the advertisement or marketing is based on Student Data or inferred from the student's online behavior or usage of the Provider's website, online service or mobile application by such student. Targeted Advertising includes advertising to a student at an online location based upon a single search query without collection and retention of a student's online activities over time. Targeted Advertising includes targeted advertising that is based upon factors, including, but not limited to, the student's recent browsing history, the student's language and the student's location. Targeted Advertising does not include advertising to a student at an online location based upon that student's current visit to that location.

Third Party: The term "Third Party" means an entity that is not the Provider or LEA.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF STUDENT DATA

LEA directs ClassDojo[Name of Company] 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 Student Data.

2. Nature of Disposition

__ Disposition shall be by destruction or deletion of Student Data, including De-Identification 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

__By *[Insert Date]*

4. Signature

_____

Authorized Representative of LEA

_____

Date

5. Verification of Disposition of Data

_____

Authorized Representative of Company

_____

OPTIONAL: EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Having robust data security policies and controls in place are the best ways to ensure data privacy. Please answer the following questions regarding the security measures in place in your organization:

1. Does your organization have a data security policy? □√ Yes □ No

2. Has your organization adopted a cybersecurity framework to minimize the risk of a data breach? If so which one(s):

____ ISO 27001/27002

__X__ CIS-20 Critical Controls

___X_ NIST Framework Improving Critical Infrastructure Security

*Currently aligning data security practices to NIST Cybersecurity Framework). "**NIST Cybersecurity Framework**" shall mean the U.S. Department of Commerce National Institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 or any later standards developed by NIST.

____ Other: _____

3. Does your organization store any Student Data outside the United States? □ Yes □ √No

4. Does your organization encrypt Student Data both in transit and at rest? □ √ Yes □ No

5. Please provide the name and contact info of your Chief Information Security Officer (CISO) or the person responsible for data security should we have follow-up questions.

Name: Dominick Bellizzi dominick@classdojo.com>
Contact information: dominick@classdojo.com

6. Please provide any additional information that you desire.
Please see our Security Whitepaper for details: https://www.classdojo.com/security/