

CLASSDOJO STUDENT DATA PRIVACY ADDENDUM¹

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”). 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 Section 1 pursuant to the ClassDojo Terms of Service located at <https://www.classdojo.com/terms> (the “Service Agreement”); and

WHEREAS, in order to provide the Services described in Section 1, 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. 6501-6502; 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.; and

WHEREAS, the documents and data transferred from LEAs and created or accessed by the Provider’s Services are also subject to various state student privacy laws; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Services and Service Agreement 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:

1. PURPOSE AND SCOPE

- 1.1. **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 its users pursuant to the Service Agreement including compliance with all applicable federal and state privacy statutes, including the FERPA, PPRA, COPPA, and IDEA. This DPA supplements the Service Agreement and together with the Service Agreement, is collectively referred to as the “Agreement”.
- 1.2. **Nature of Services Provided.** Pursuant to and as fully described in the Service Agreement, Provider has agreed to provide the digital educational services as set forth in Exhibit “A” hereto and any other products and services that Provider may provide now or in the future (the “Services”).
- 1.3. **Student Data to Be Provided.** In order to perform the Services, the Parties shall indicate the categories of Student Data to be provided or collected by the Provider in the Schedule of Data, attached hereto as Exhibit “B”.
- 1.4. **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.

2. DATA OWNERSHIP AND AUTHORIZED ACCESS

- 2.1. **Student Data Property of LEA.** All Student Data or any other Education Records (as defined on Exhibit “C”) transmitted to the Provider pursuant to this Agreement is and will continue to be the

¹ Modeled After The Student Data Privacy Consortium’s Set Of Baseline Model Clauses

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 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 Education Records covered per this Agreement shall remain the exclusive property of the LEA or the party who provided such data (such as the student or parent).

- 2.2. **Exemptions under FERPA.** LEA may not generally disclose Personally Identifiable Information from an eligible student's Education Record 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 exemption for Directory Information ("Directory Information Exemption") or 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. Additionally, certain information, provided to Provider by LEA about a student, such as student name and grade level, may be considered Directory Information (as defined on Exhibit "C") under FERPA and thus not an Education Record.
- 2.3. **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, consistent with the functionality of Services. Provider shall cooperate and respond within thirty (30) 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, provided however, that Provider may also allow for direct access requests (but not correction or deletion rights) of Student Data and/or Education Records from a verified parent.
- 2.4. **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. Additionally, If Student Generated Content is stored or maintained by the Provider as part of the Services, Provider may, at the request or with the consent of the 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.
- 2.5. **Third Party Request.** Should a third party, excluding a Service Provider, 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) if Provider believes in good faith that such disclosure is necessary to protect the rights, property or personal safety of Provider's users, employees or others. Provider shall notify the LEA in advance of a compelled disclosure to a third party, unless legally prohibited.

- 2.6. **Service Providers.** Provider shall enter into written agreements with all Service Providers performing functions pursuant to this Agreement, whereby the Service Providers agree to protect Student Data in manner no less stringent than the terms of this DPA. The list of Provider's current Service Providers can be accessed through the Provider's Privacy Policy (which may be updated from time to time).

3. DUTIES OF LEA

- 3.1. **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, and IDEA. If LEA is providing Directory Information or any Education Record to Provider, LEA represents, warrants and covenants to Provider, as applicable, that LEA has:
- a. 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
 - b. 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
 - 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.

- 3.2. **Reasonable Security.** LEA shall employ administrative, physical, and technical safeguards consistent with industry standards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted data from unauthorized access, disclosure or acquisition by an unauthorized person.
- 3.3. **Unauthorized Access Notification.** LEA shall notify Provider immediately, but in no less than 72 hours, 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.

4. DUTIES OF PROVIDER

- 4.1. **Privacy Compliance.** The Provider shall comply in all material respects with all applicable state and federal laws and regulations pertaining to data privacy and security, applicable to the Provider in providing the Service to LEA. With respect to Student Data that the LEA permits Provider to collect or access pursuant to the Agreement, Provider agrees to support LEA in upholding LEA's responsibilities with FERPA and PPRA.
- 4.2. **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. The foregoing limitation does not apply to any De-Identified Data (as defined in Exhibit "C").
- 4.3. **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.

- 4.4. **No Disclosure.** Provider shall not disclose, transfer, share or rent any Student Data obtained under the Agreement in a manner that directly identifies an individual student to any other entity other than LEA, except: (i) as authorized by the Agreement; (ii) as directed by LEA; (iii) to authorized users of the Services, including parents or legal guardians; (iv) as permitted by law; (v) in response to a judicial order as set forth in Section 2.5; (vi) to protect the safety or integrity of users or others, or the security of the Services; or (vii) to Service Providers, in connection with operating or improving the Service. Provider will not Sell (as defined in Exhibit "C") Student Data to any third party.
- 4.5. **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 Data and not to transfer De-identified Data to any party unless that party agrees in writing not to attempt re-identification.
- 4.6. **Disposition of Data.** Provider shall, at LEA's request, dispose of or delete all Personally Identifiable Information contained in Student Data within a reasonable time period following a written request. 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 the Agreement 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 to retain Student 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 contained in Student Data to make it unreadable or indecipherable or De-Identified or placed in a separate student account, pursuant to the other terms of the DPA. Provider shall provide written notification to LEA when the Personally Identifiable Information contained in Student Data has been disposed pursuant to the LEA's request for deletion. The duty to dispose of Student Data shall not extend to data that has been De-Identified. The LEA may employ a "Request for Return or Deletion of Student Data" substantially in the form attached hereto as Exhibit "D".
- 4.7. **Transfer of Student Data to LEA.** If a written request is received from LEA to transfer Personally Identifiable Information contained in Student Data to LEA, Provider shall transfer said Personally Identifiable Information contained in Student Data to LEA or LEA's designee within sixty (60) days of the date of such written request by LEA, or as required by law, and according to a schedule and procedure as the Parties may reasonably agree.
- 4.8. **Advertising Prohibition.** Provider is prohibited from using Personally Identifiable Information contained in Student Data to (a) serve Targeted Advertising to students or families/guardians unless with the consent of parent/guardian or LEA; (b) develop a profile of a student for any commercial purpose other than providing the Service or as authorized by the parent/guardian or LEA; or (c) develop commercial products or services, other than as necessary to provide the Service to LEA, as authorized by the parent or legal guardian, or as permitted by applicable law. This section shall not be construed to (i) limit the ability of Provider to use Student Data for adaptive learning or customized student learning purposes (including generating personalized learning recommendations for account holders or sending Program Communications to account holders); (ii) prohibit Provider from using aggregate or De-Identified Data to inform, influence or enable marketing, advertising or other commercial efforts by Provider, (iii) prohibit Provider from marketing or advertising directly to

parents or other users so long as the marketing or advertising did not result from the use of Personally Identifiable Information contained in Student Data obtained by Provider from providing the Services; (iv) prohibit Provider from using Student Data to recommend educational products or services to parents/guardians, students or LEA's so long as the recommendations are not based in whole or part by payment or other consideration from a third party; (v) apply to the marketing of school memorabilia such as photographs, yearbooks, or class rings or (vi) prohibit Provider from using Student Data with parent/guardian consent to direct advertising to students to identify higher education or scholarship providers that are seeking students who meet specific criteria.

5. DATA SECURITY AND DATA BREACH

5.1. 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, including when transmitting and storing such information. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "E" 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 consistent with Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees, contractors or Service Providers that are performing the Services.
- b. **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 provide the Service, to fulfill data requests by LEA or as otherwise set forth in the Agreement. The foregoing does not limit the ability of the Provider to disclose information as permitted under Section 2.5 or to allow any necessary Service Providers to view or access data as set forth in Section 4.4.
- c. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the Services.
- d. **Security Technology.** When the Service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology shall be employed to protect Student Data from unauthorized access. The security measures employed shall include server authentication and data encryption at rest and in transit. Provider shall host Student Data pursuant to the Agreement in an environment using a firewall that is maintained according to industry standards.
- e. **Security Coordinator.** The name and contact information of each Party's designated representative for the purposes of matters relating to security of Student Data received pursuant to the Agreement is set forth below:
 - i. Provider's security coordinator ("Security Coordinator") is: Elisette Weiss, Privacy Operations, elisette@classdojo.com.
 - ii. LEA's designated representative of matters relating to security of Student Data is set forth on the signature page of this DPA.
- f. **Service Provider Bound.** Provider shall enter into written agreements whereby Service Providers agree to secure and protect Student Data in a manner no less stringent than the terms of this Section 5. Provider shall periodically conduct or review compliance monitoring and assessments of Service Providers to determine their compliance with this Section 5.

- g. **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.

5.2. **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 as required by the applicable state law, but in no event later than 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,” “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 5.2(a) shall include such information required by the applicable state law, and at a minimum, the following information, to the extent available:
 - i. The name and contact information of the reporting Provider subject to this section.
 - ii. A list of the types of Personally Identifiable Information that were or are reasonably believed to have been the subject of the Security Incident.
 - iii. 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.
 - iv. Whether, to the knowledge of Provider at the time the Security Incident Notice was provided the notification was delayed as a result of a law enforcement investigation
 - v. A general description of the Security Incident, if that information is possible to determine at the time the notice is provided.
- c. At Provider’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 breached 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 applicable State and 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 involving 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 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.

6. MISCELLANEOUS

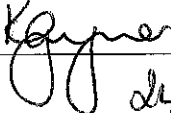
- 6.1. **Term.** The Provider shall be bound by this DPA for the duration of the Service Agreement or as required by law.
- 6.2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by terminating the Service Agreement as set forth therein. The LEA or Provider may terminate this DPA and the Service Agreement in the event of a material breach of the terms of this DPA.
- 6.3. **Effect of Termination Survival.** If the Service Agreement is terminated (thereby terminating this DPA), the Provider shall dispose of all of LEA's Personally Identifiable Information contained in Student Data following the procedures set forth in Section 4.6, which includes De-Identification.
- 6.4. **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, including, without limitation, any license rights, limitation of liability or indemnification provisions.
- 6.5. **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 before:
- a. The designated representative for the Provider for this DPA is: Elisette Weiss, Privacy Operations, ClassDojo, Inc. elisette@classdojo.com
 - b. The designated representative for the LEA for this DPA is the individual who enters into the DPA and provides his or her relevant email address (online) during the acceptance process.
- 6.6. **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. For clarity, nothing in this Section prohibits Provider from amending the Service Agreement pursuant to the amendment provisions set forth therein.
- 6.7. **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.

- 6.8. **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 THE LEA RESIDES IN, OF THE STATE OF THE LEA SIGNING THE DPA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
- 6.9. **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.
- 6.10. **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.
- 6.11. **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.
7. **INTERNATIONAL DATA PROTECTION REGULATIONS AND ADDENDUM.** For additional provisions relating to international data protection regulations and obligations (including the General Data Protection Regulation (GDPR)) please contact intdpa@classdojo.com for the ClassDojo International Data Protection Addendum.

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: Warwickshire (Paddox Primary)
Address: Fareham Avenue, Rugby.
Country: A.B.
LEA Authorized Representative full name: Kate Guymer
Title: Headteacher
Email: head2625@welearn365.com
LEA Authorized Representative signature: 
Date: 24.11.22

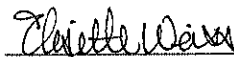
Per section 2.3, LEA's contact for parent inquiries:

Name & Email: guymer.k1@welearn365.com
Title: Headteacher

Per section 5.1(e) LEA's designated representative of matters relating to security of Student Data:

Name & Email: aldridge.s@welearn365.com
Title: Resource Director

ClassDojo Representative signature:



Authorized Representative full name:

Elisette Weiss

Title:

District Partnerships & Privacy Operations

Email:

privacy@classdojo.com

Address:
U.S.A

735 Tehama Street, San Francisco, CA,

Date:

December 16, 2020

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 options through its platform:

- Communication tools to help teachers, students, and parents connect with each other
- A way for teachers to give feedback and assignments to students, and other classroom management tools
- A way for teachers to share photos, videos, files, and more from the classroom for parents and students to see
- Student portfolios, where students can share their work with teachers and parents can upload content
- 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.

The Service shall not include any Outside School Accounts. 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 (as defined in the Student DPA) shall not include information a student or parent provides to ClassDojo through such Outside School Accounts independent of the student’s or parent’s engagement with the Services at the direction of the school or controller.

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)	✓ Not from students, unless they message directly with their teacher in Portfolios
Biometric Data	Physical or behavioral human characteristics to can be used to identify 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 <i>For ClassDojo: "Feedback points" are added by the student's teacher</i>	✓
Demographics	Date of Birth <i>For ClassDojo: This is collected as an age, not DOB</i>	✓
	Place of Birth	N/A
	Gender <i>For ClassDojo: We ask adults for an optional Mr./Miss/etc. salutation</i>	✓ not from students
	Ethnicity or race	N/A
	Language information (native, preferred or primary language spoken by student) <i>For ClassDojo: This is obtained via browser/device preferences</i>	✓
	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 <i>For ClassDojo: option to only share last initial</i>	✓
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. <i>For ClassDojo: this may also be teacher assigned projects</i>	✓
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-party-service-providers/>

EXHIBIT “C”
DEFINITIONS

“De-Identified Data” means information that has all Personally Identifiable Information, including direct and indirect identifiers removed or obscured, such that the remaining information does not reasonably identify an individual. This includes, but is not limited to, name, date of birth, demographic information, location information and school identity.

“Directory Information” shall have the meaning set forth under FERPA cited as 20 U.S.C. 1232 g(a)(5)(A).

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

“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” shall mean the National Institute of Standards and Technology (“NIST”) Special Publication 800-63-3 Digital Authentication Guideline.

“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. 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.

“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. Beyond School) offered through the Services or ClassDojo website or application.

“Sell” consistent with the Student Privacy Pledge, does not include or apply to a purchase, merger or other type of acquisition of a company by another entity, provided that the company or successor entity continues to treat the Personally Identifiable Information contained in Student Data in a manner consistent with this DPA with respect to the previously acquired Personally Identifiable Information contained in Student Data. Sell also does not include sharing, transferring or disclosing Student Data with a Service Provider that is necessary to perform a business purpose (such as detecting security incidents, debugging and repairing, analytics, storage or other processing activities) provided that the Service Provider does not Sell the Student Data except as necessary to perform the business purpose. Provider is also not “selling” personal information (i) if a user directs Provider to intentionally disclose Student Data or uses ClassDojo to intentionally interact with a third party, provided that such third party also does not Sell the Student Data; or (ii) if a parent or other user (with parent consent) purchases Student Data (e.g. enhanced classroom reports or photos).

“Service Provider” 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 Services, and who has access to PII.

“School Official” means for the purposes of this DPA and pursuant to FERPA (34 CFR 99.31 (B)), 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 Education Records.

“Student Data” means 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 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, student identifies, search activity, photos, voice recordings or geolocation information. To the extent U.S. law applies, Student Data may include Education Records. 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.

“Student Generated Content” means materials or content created by a student including content created at the direction of the LEA personnel or during classroom use of the Services, such as, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content. “Student Generated Content” does not include student responses to a standardized assessment where student possession and control would jeopardize the validity and reliability of that assessment.

“Targeted Advertising” means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the Provider’s website, online service or mobile application by such student or the retention of such student’s online activities or requests over time and across non-affiliate websites for the purpose of targeting subsequent advertising. This does not include advertising to a student based on the content of a web page, search query or a user’s contemporaneous behavior on the website or a response to a student’s response or request for information or feedback, both of which are permitted.

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF STUDENT DATA

LEA directs ClassDojo 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]

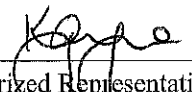
3. Timing of Disposition

Student Data shall be disposed of by the following date:

☒ As soon as commercially practicable

☐ By *[Insert Date]*

4. Signature



Authorized Representative of LEA

24.11.22

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT “E”
DATA SECURITY REQUIREMENTS

Please see our Security Whitepaper for details: <https://www.classdojo.com/security/>

CLASSDOJO INTERNATIONAL DATA PROCESSING ADDENDUM

(Revision August 2020)

This International Data Processing Addendum, including its Schedules and Appendices, (“**Int. DPA**”) forms part of the Service Agreement or other written or electronic agreement between ClassDojo, Inc. and LEA for the online services from ClassDojo, as well as the Student Data Protection Addendum (“**Student DPA**”), which includes the services listed on Appendix 3 to the Standard Contractual Clauses of this Int. DPA (identified either as “**Services**” or otherwise in the applicable agreement, and hereinafter defined as “**Services**”) (collectively, the “**Agreement**”) to reflect the parties’ agreement with regard to the Processing of Personal Data.

By signing the Agreement, LEA enters into this Int. DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, in the name and on behalf of its Authorized Affiliates, if and to the extent ClassDojo processes Personal Data for which such Authorized Affiliates qualify as the Controller. For the purposes of this Int. DPA only, and except where indicated otherwise, the term “**LEA**” shall include LEA and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning set forth in the Agreement.

In the course of providing the Services to LEA pursuant to the Agreement, ClassDojo may Process Personal Data on behalf of LEA and the Parties agree to comply with the following provisions with respect to any Personal Data.

HOW TO EXECUTE THIS EU DPA:

1. This Int. DPA consists of two parts: the main body of the Int. DPA, and Schedules 1, 2, and 3 (including Appendices 1 to 3).
2. This Int. DPA has been pre-signed on behalf of ClassDojo. The Standard Contractual Clauses in Schedule 3 have been pre-signed by ClassDojo, Inc. as the data importer.
3. To complete this Int. DPA, LEA must:
 - a. Complete the information in the signature box and sign on Page 5.
 - b. Send the signed DPA to ClassDojo by email to intdpa@classdojo.com indicating, if applicable, the LEA’s Account Number.

Upon receipt of the validly completed Int. DPA by ClassDojo as indicated above, this Int. DPA will become legally binding.

For the avoidance of doubt, signature of the Int. DPA on page 5 shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices. Where LEA wishes to separately execute the Standard Contractual Clauses and its Appendices, LEA should also complete the information as the data exporter on Page 8 and complete the information in the signature box and sign on Pages 12, 13, and 14.

HOW THIS DPA APPLIES

If the LEA entity signing this Int. DPA is a party to the Agreement, this Int. DPA is an addendum to and forms part of the Agreement. This Int. DPA shall not replace any comparable or additional rights relating to Processing of LEA Data contained in LEA’s Agreement (including any existing data processing addendum to the Agreement (e.g. the Student DPA)).

DATA PROCESSING TERMS

1. DEFINITIONS

“**Affiliate**” means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. “**Control**,” for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

“**Authorized Affiliate**” means any of LEA’s Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between LEA and ClassDojo, but has not signed its own Terms of Service or Agreement with ClassDojo and is not a “**LEA**” as defined under this DPA.

“**CCPA**” means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.*, and its implementing regulations.

“**Controller**” means the entity which determines the purposes and means of the Processing of Personal Data.

“**LEA**” means the entity that executed the Agreement together with its Affiliates (for so long as they remain Affiliates) which have signed the DPA and Service Agreement.

“LEA Data” means what is defined in the Agreement as “LEA Data”, “Student Data”, “User Content”, or “Your Data, provided that such data is electronic data and information submitted by or for LEA (or collected by ClassDojo and Processed on behalf of LEA) to the Services.

“Data Protection Laws and Regulations” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its states, applicable to the Processing of Personal Data under the Agreement.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“Data Subject Rights” means all rights granted to Data Subjects by Data Protection Laws and Regulations, including the right to information, access, rectification, erasure, restrictions, portability, objection, and not to be subject to automated decision-making.

“GDPR” means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“Personal Data” means any information relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data or personally identifiable information under applicable Data Protection Laws and Regulations), where for each (i) or (ii), such data is LEA Data.

“Personnel” means any natural person acting under the authority of ClassDojo.

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity which Processes Personal Data on behalf of the Controller, including as applicable any “service provider” as that term is defined by the CCPA.

“Security and Privacy Documentation” means the Security and Privacy Documentation applicable to the Services, as updated from time to time, and accessible via ClassDojo’s webpage at <https://www.classdojo.com/security/> or as otherwise made reasonably available by ClassDojo.

“ClassDojo” means the ClassDojo entity which is a party to this Int. DPA, as specified in the section “HOW THIS DPA APPLIES” above, being ClassDojo, Inc., a company incorporated in Delaware, United States

“ClassDojo Group” means ClassDojo and its Affiliates engaged in the Processing of Personal Data.

“Standard Contractual Clauses” means the agreement executed by and between LEA and ClassDojo and attached hereto as Schedule 3 pursuant to the European Commission’s decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

“Sub-processor” means any Processor engaged by ClassDojo or a member of the ClassDojo Group.

“Supervisory Authority” means an independent public authority which is established by an EU Member State pursuant to the GDPR.

2. PROCESSING OF PERSONAL DATA

2.1 Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, LEA is the Controller, ClassDojo is the Processor and that ClassDojo or members of the ClassDojo Group will engage Sub-processors pursuant to the requirements set forth in Section 5 “Sub-processors” below.

2.2 LEA’s Processing of Personal Data. LEA shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of ClassDojo as Processor. For the avoidance of doubt, LEA’s instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations. LEA shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which LEA acquired (or instructed ClassDojo to acquire on its behalf) Personal Data. LEA specifically acknowledges that its use of the Services will not violate the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under the CCPA or other Data Protection Laws and Regulations.

2.3 ClassDojo’s Processing of Personal Data. ClassDojo shall Process Personal Data on behalf of and only in accordance with LEA’s documented instructions for the following purposes: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Users in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by LEA (e.g., via email) where such instructions are consistent with the terms of the Agreement and issued by LEA’s management board, data protection officers or the manager of the LEA’s legal department, as applicable.

- 2.4 Details of the Processing.** The subject-matter of Processing of Personal Data by ClassDojo is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this Int. DPA are further specified in Schedule 2 (Details of the Processing) to this Int. DPA.

3. ASSISTANCE

- 3.1** ClassDojo must provide reasonable assistance to LEA with the fulfilment of LEA's own obligations under Data Protection Laws and Regulations with respect to: 1) complying with Data Subjects' requests to exercise Data Subject Rights, 2) replying to inquiries or complaints from Data Subjects, 3) replying to investigations and inquiries from Supervisory Authorities, 4) notifying LEA of LEA Data Incident (as defined below) relating to LEA's Student Data, and 5) prior consultations with Supervisory Authorities. ClassDojo will follow the procedures set forth in Section 2.3 ("**Parent Access**") of the Student DPA.
- 3.2** Upon reasonable request, ClassDojo must provide LEA with all information necessary to enable LEA to satisfy notification obligations, maintaining records of Processing activities, or performing a data protection impact assessment.
- 3.3** ClassDojo must promptly inform LEA if ClassDojo believes that an instruction of LEA violates Data Protection Laws and Regulations.
- 3.4** Unless prohibited by EU or EU member state law, and subject to the procedures set forth in Section 2.5 of the Student DPA ("**Third-Party Request**"), ClassDojo must promptly inform LEA if ClassDojo receives a request to disclose Personal Data from law enforcement, courts or any government entity; is subject to a legal obligation that requires ClassDojo to Process Personal Data in contravention of LEA's instructions; or is otherwise unable to comply with Data Protection Laws and Regulations or this Int. DPA. If ClassDojo is prevented from notifying LEA as required under this Int. DPA, ClassDojo must consult and comply with the instructions of the competent Supervisory Authority.

4. ClassDojo PERSONNEL

- 4.1 Training and Access.** ClassDojo must implement appropriate technical and organizational measures to ensure that Personnel do not Process Personal Data except on the instructions of the LEA and will follow additional obligations as set forth in Section 4.3 of the Student DPA ("**Employee Obligations**"), Section 5.1(a) of the Student DPA ("**Passwords and Employee Access**"), and Section 5.1 (d) of the Student DPA ("**Employee Training**").
- 4.2 Confidentiality.** ClassDojo must keep all LEA Data and any information relating to the Processing thereof, in strict confidence as set forth in Section 4.4 of the Student DPA ("**No Disclosure**").

5. SUB-PROCESSORS

- 5.1 Appointment of Sub-processors.** LEA acknowledges and agrees that (a) ClassDojo Affiliates may be retained as Sub-processors; and (b) ClassDojo and ClassDojo's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. LEA hereby authorizes ClassDojo to engage the Sub-processors listed as a link from ClassDojo's Privacy Policy (which may be updated from time to time). ClassDojo or a ClassDojo Affiliate has entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in the Agreement with respect to the protection of LEA Data to the extent applicable to the nature of the Services provided by such Sub-processor. Provider must obtain sufficient guarantees from all Sub-processors that they will implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Data Protection Laws and Regulations and this Int. DPA.
- 5.2 List of Current Sub-processors and Notification of New Sub-processors.** ClassDojo shall make available to LEA the current list of Sub-processors for the Services identified in Appendix 3 of the Standard Contractual Clauses attached hereto. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location ("**Sub-processor Documentation**"). LEA may also find the Sub-Processor Documentation within ClassDojo's website in its Privacy Policy under "Service Providers" or linked directly here: <https://www.classdojo.com/third-party-service-providers/>. LEA may send an email to subprocessornotification@classdojo.com to subscribe to receive notification of a new Sub-processor. If LEA subscribes, ClassDojo will provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.
- 5.3 Objection Right for New Sub-processors.** LEA may object to ClassDojo's use of a new Sub-processor by notifying ClassDojo promptly in writing within thirty (30) days after receipt of ClassDojo's notice in accordance with the mechanism set out in Section 5.2. In the event LEA objects to a new Sub-processor, as permitted in the preceding sentence, ClassDojo will use reasonable efforts to make available to LEA a change in the Services or recommend a commercially reasonable change to LEA's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening LEA. If ClassDojo is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, LEA may terminate the Agreement with respect to only to those

Services which cannot be provided by ClassDojo without the use of the objected-to new Sub-processor by providing written notice to ClassDojo. ClassDojo will refund LEA any prepaid fees (if applicable) covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on LEA.

- 5.4 Liability.** ClassDojo shall be liable for the acts and omissions of its Sub-processors to the same extent ClassDojo would be liable if performing the services of each Sub-processor directly under the terms of this EU DPA, except as otherwise set forth in the Agreement.

6. SECURITY

- 6.1 Controls for the Protection of LEA Data.** ClassDojo shall maintain appropriate technical and organizational measures for protection of the security appropriate to the risk presented by the Processing (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, LEA Data), confidentiality and integrity of LEA Data, as set forth in Section 5 of the Student DPA ("Data Security") as well as the Security and Privacy Documentation. ClassDojo regularly monitors compliance with these measures. ClassDojo will not materially decrease the overall security of the Services during a subscription term.

7. LEA DATA INCIDENT MANAGEMENT AND NOTIFICATION

ClassDojo shall notify LEA without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to LEA Data, including Personal Data, transmitted, stored or otherwise Processed by ClassDojo or its Sub-processors of which ClassDojo becomes aware (a "**LEA Data Incident**"). ClassDojo shall make reasonable efforts to identify the cause of such LEA Data Incident and take those steps as ClassDojo deems necessary and reasonable in order to remediate the cause of such a LEA Data Incident to the extent the remediation is within ClassDojo's reasonable control. The obligations herein shall not apply to incidents that are caused by LEA or LEA's Users.

8. RETURN AND DELETION OF LEA DATA

ClassDojo shall return LEA Data to LEA and, to the extent allowed by applicable law, delete LEA Data in accordance with the procedures and timeframes specified in Section 4.6 ("**Disposition of Data**") of the Student DPA.

9. AUTHORIZED AFFILIATES

- 9.1 Contractual Relationship.** The parties acknowledge and agree that, by executing the Agreement, LEA enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between ClassDojo and each such Authorized Affiliate subject to the provisions of the Agreement and this Section 9 and Section 10. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement and is only a party to the DPA. All access to and use of the Services and Content by Authorized Affiliates must comply with the terms and conditions of the Agreement and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by LEA.
- 9.2 Communication.** The LEA that is the contracting party to the Agreement shall remain responsible for coordinating all communication with ClassDojo under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.
- 9.3 Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to the DPA with ClassDojo, it shall to the extent required under applicable Data Protection Laws and Regulations be entitled to exercise the rights and seek remedies under this DPA, subject to the following:
- 9.3.1** Except where applicable Data Protection Laws and Regulations require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against ClassDojo directly by itself, the parties agree that (i) solely the LEA that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the LEA that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below).
- 9.3.2** The parties agree that the LEA that is the contracting party to the Agreement shall, when carrying out an on-site audit of the procedures relevant to the protection of Personal Data, take all reasonable measures to limit any impact on ClassDojo and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this EU DPA, and all EU DPAs between Authorized Affiliates and ClassDojo, whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' section of the Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, ClassDojo's and its Affiliates' total liability for all claims from LEA and all of its Authorized Affiliates arising out of or related to the Agreement and all EU DPAs shall apply in the aggregate for all claims under both the Agreement and all EU DPAs established under the Agreement, including by LEA and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to LEA and/or to any Authorized Affiliate that is a contractual party to any such DPA.

11. EUROPEAN SPECIFIC PROVISIONS

11.1 GDPR. ClassDojo will Process Personal Data in accordance with the GDPR requirements directly applicable to SFDC's provision of its Services.

11.2 Transfer mechanisms for data transfers. Subject to the additional terms in Schedule 1, ClassDojo makes available the transfer mechanisms listed below which shall apply, in the order of precedence as set out in Section 11.3, to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws and Regulations:

1. The Standard Contractual Clauses set forth in Schedule 3 to this Int. DPA apply to the Services listed in Appendix 3 to the Standard Contractual Clauses (the "SCC Services"), subject to the additional terms in Section 3 of Schedule 1; and
2. Where applicable, pursuant to GDPR Art. 49 derogations for the transfer of personal data, such as consent or performance of a contract.

11.3 Order of precedence. In the event that Services are covered by more than one transfer mechanism, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (1) (1) Art. 49 derogations (e.g. consent), and (2) the Standard Contractual Clauses.

12. LEGAL EFFECT

This DPA shall only become legally binding between LEA and ClassDojo when the formalities steps set out in the Section "HOW TO EXECUTE THIS DPA" above have been fully completed.

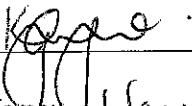
List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers

Schedule 2: Details of the Processing

Schedule 3: Standard Contractual Clauses

The parties' authorized signatories have duly executed this DPA:

Signature: 

LEA Legal Name: Warwickshire

Print Name: Kate Guymer

Title: Headteacher

Date: 24.11.22

SCHEDULE 1 - TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

1. ADDITIONAL TERMS FOR SCC SERVICES

- 1.1. **LEAs covered by the Standard Contractual Clauses.** The Standard Contractual Clauses and the additional terms specified in this Section 2 apply to (i) LEA which is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom and, (ii) its Authorized Affiliates. For the purpose of the Standard Contractual Clauses and this Section 2, the aforementioned entities shall be deemed "data exporters".
- 1.2. **Instructions.** This DPA and the Agreement are LEA's complete and final documented instructions at the time of signature of the Agreement to ClassDojo for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of Clause 5(a) of the Standard Contractual Clauses, the following is deemed an instruction by the LEA to process Personal Data: (a) Processing in accordance with the Agreement; (b) Processing initiated by Users in their use of the SCC Services and (c) Processing to comply with other reasonable documented instructions provided by LEA (e.g., via email) where such instructions are consistent with the terms of the Agreement.
- 1.3. **Appointment of new Sub-processors and List of current Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, LEA acknowledges and expressly agrees that (a) ClassDojo and ClassDojo's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the SCC Services. ClassDojo shall make available to LEA the current list of Sub-processors in accordance with Section 5.2 of this Int. DPA
- 1.4. **Notification of New Sub-processors and Objection Right for new Sub-processors.** Pursuant to Clause 5(h) of the Standard Contractual Clauses, LEA acknowledges and expressly agrees that ClassDojo may engage new Sub-processors as described in Sections 5.2 and 5.3 of the Int. DPA.
- 1.5. **Copies of Sub-processor Agreements.** The parties agree that the copies of the Sub-processor agreements that must be provided by ClassDojo to LEA pursuant to Clause 5(j) of the Standard Contractual Clauses may have all commercial information, or clauses unrelated to the Standard Contractual Clauses or their equivalent, removed by ClassDojo beforehand; and, that such copies will be provided by ClassDojo, in a manner to be determined in its discretion, only upon request by LEA.
- 1.6. **Audits and Certifications.** The parties agree that the audits described in Clause 5(f) and Clause 12(2) of the Standard Contractual Clauses shall be carried out in accordance with the following specifications:

Upon LEA's request, and subject to any appropriate confidentiality agreements being executed, ClassDojo shall make available to LEA that is not a competitor of ClassDojo (or LEA's independent, third-party auditor that is not a competitor of ClassDojo) information regarding ClassDojo's compliance with the obligations set forth in this DPA in the form of the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation to the extent ClassDojo makes them generally available to its LEAs. LEA may contact ClassDojo in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of Personal Data. LEA shall reimburse ClassDojo for any time expended for any such on-site audit. Before the commencement of any such on-site audit, LEA and ClassDojo shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which LEA shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by ClassDojo. LEA shall promptly notify ClassDojo with information regarding any non-compliance discovered during the course of an audit.
- 1.7. **Certification of Deletion.** The parties agree that the certification of deletion of Personal Data that is described in Clause 12(1) of the Standard Contractual Clauses shall be provided by ClassDojo to LEA only upon LEA's request.
- 1.8. **Conflict.** In the event of any conflict or inconsistency between the body of this DPA and any of its Schedules (not including the Standard Contractual Clauses) and the Standard Contractual Clauses in Schedule 3, the Standard Contractual Clauses shall prevail.

SCHEDULE 2 - DETAILS OF THE PROCESSING

Nature and Purpose of Processing

ClassDojo will Process Personal Data as necessary to perform the SCC Services pursuant to the Agreement, and as further instructed by LEA in its use of the SCC Services.

Duration of Processing

Subject to Section 8 of the Int. DPA, ClassDojo will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

Categories of Data Subjects

LEA may submit Personal Data to the SCC Services (or ClassDojo may collect and Process on behalf of LEA), the extent of which is determined and controlled by LEA in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Employees, agents, advisors, freelancers of LEA (who are natural persons)
- LEA's Users authorized by LEA to use the Services (who are natural persons)

Type of Personal Data

LEA may submit Personal Data to the SCC Services (or ClassDojo may collect and Process on behalf of the LEA), the extent of which is determined and controlled by LEA in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

[See Schedule of Data attached to the Student Data DPA]

Special categories of data (if appropriate)

LEA shall not provide any special categories of Personal Data to the SCC Services and which is for the sake of clarity Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

SCHEDULE 3 - STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

Name of the data exporting organisation: _____

Address: _____

Tel.: _____ fax: _____ e-mail: _____

Other information needed to identify the organisation: _____

.....
(the data **exporter**)

And

Name of the data importing organisation: **ClassDojo, Inc.**

Address: **735 Tehama Street, San Francisco, CA 94103, USA**

e-mail: **privacy@classdojo.com**

Other information needed to identify the organisation: Not applicable

(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses: 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

- (a) '*the data exporter*' means the controller who transfers the personal data;
- (b) '*the data importer*' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (c) '*the subprocessor*' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (d) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- (e) '*technical and organisational security measures*' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

- 1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- 2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- 3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
- 4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.
- 5.

Clause 4

Obligations of the data exporter

The data importer agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer

to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5 ***Obligations of the data importer***

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10
Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11
Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
2. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
3. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): Kate Anyue Position: Headteacher

Address: Paddox Primary School, Fareham Ave, Rugby

Other information necessary in order for the contract to be binding (if any):

**PADDOX PRIMARY
SCHOOL
FAREHAM AVENUE
RUGBY CV22 5HS
01788 572340**

Signature: [Signature] (stamp of organisation)

On behalf of the data importer:

Name (written out in full): Elisette Weiss Position: District Partnerships & Privacy Operations

Address: 735 Tehama Street, San Francisco, CA 94103

Other information necessary in order for the contract to be binding (if any):

Signature: [Signature] (stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is the legal entity specified in Section 3.1 of Schedule 1 of the DPA.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

ClassDojo, Inc. is a provider of education technology and a school communication platform that helps bring teachers, school leaders, families, and students together, which processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the SCC Services (or ClassDojo may collect and Process on behalf of the Data exporter), the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Employees, agents, advisors, freelancers of data exporter (who are natural persons)
- Data exporter's Users authorized by data exporter to use the Services (who are natural persons)

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the SCC Services (or ClassDojo may collect and Process on behalf of the Data exporter), the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- Please see the Schedule of Data attached to the Agreement

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Data exporter shall not submit special categories of data to the SCC Services.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the SCC Services pursuant to the Agreement.

DATA EXPORTER

Name: Kate Anyue

Authorised Signature Kate Anyue

DATA IMPORTER

Name: Elisette Weiss on behalf of ClassDojo, Inc.

Authorised Signature Elisette Weiss

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

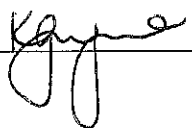
This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Data importer will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the SCC Services, as described in the Security and Privacy Documentation, and accessible via [http:// https://www.classdojo.com/security/](http://https://www.classdojo.com/security/) or otherwise made reasonably available by data importer. Data Importer will not materially decrease the overall security of the SCC Services during a subscription term.

DATA EXPORTER

Name: Kate Guyne

Authorised Signature: 

DATA IMPORTER

Name: Elisette Weiss, on behalf of ClassDojo, Inc.

Authorised Signature: 

APPENDIX 3 TO THE STANDARD CONTRACTUAL CLAUSES

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

ClassDojo provides the following options through its platform:

- Communication tools to help teachers, students, and parents connect with each other
- A way for teachers to give feedback and assignments to students, and other classroom management tools
- A way for teachers to share photos, videos, files, and more from the classroom for parents and students to see
- Student portfolios, where students can share their work with teachers and parents can upload content
- 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.

The Service shall not include any Outside School Accounts. 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 (as defined in the Student DPA) shall not include information a student or parent provides to ClassDojo through such Outside School Accounts independent of the student's or parent's engagement with the Services at the direction of the school or controller.