MASSACHUSETTS STUDENT DATA PRIVACY AGREEMENT VERSION (2020)

Wayland Public Schools

and

Artsonia LLC

August 19, 2020

This Massachusetts Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Wayland Public Schools (hereinafter referred to as "LEA") and Artsonia LLC (hereinafter referred to as "Provider") on August 19, 2020. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed or will agree to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") as described in Article I and Exhibit "A"; and

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

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

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

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

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

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data (as defined in Exhibit "C") transmitted to Provider from the LEA pursuant to Exhibit "A", including compliance with all applicable state privacy statutes, including the FERPA, PPRA, COPPA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In performing these services, to the extent Personally Identifiable Information (as defined in Exhibit "C") from Pupil Records (as defined in Exhibit "C") are transmitted to Provider from LEA, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA as it pertains to the use of Student Data. Control duties are set forth below.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described in Exhibit "A".

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

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in all other writings, including, but not limited to, a service agreement, privacy policies or any terms of service.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or any other Pupil Records transmitted to the Provider pursuant to this Agreement is and will continue to be the property of and under the control of the LEA , or to the party who provided such data (such as the student or parent.). The Provider further acknowledges and agrees that all copies of such Student Data or any other Pupil 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 Pupil Records. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per this Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA and state law, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. The Provider will cooperate and provide Student Data within ten (10) days at the LEA's request. In responding to such a request, Provider may transfer Pupil-Generated Content to a separate account, according to the procedures set forth below.

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

3. **Separate Account**. Provider shall, at the request of the LEA, transfer Student Generated Content to a separate student account.

4. **Third Party Request**. Should a Third Party, 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 and shall cooperate with the LEA to collect the required information, unless and to the extent that the 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; or (iii) to enforce the Agreement. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited. Except as otherwise permitted by this DPA, including as described in Exhibit A, or as authorized by a parent or legal guardian, the Provider will not use, disclose, compile, transfer, sell the Student Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Student Data and/or any portion thereof, without the express written consent of the LEA or without a court order or lawfully issued subpoena. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

5. **No Unauthorized Use**. Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified to provide the Services in this DPA.

6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to this DPA, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With Laws**. LEA shall provide Student Data for the purposes of the DPA in compliance with any applicable state or federal laws and regulations pertaining to data privacy and security, including, without limitation the FERPA, PPRA, IDEA, 603 C.M.R. 23.00, 603 CMR 28.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H, and the other privacy statutes quoted in this DPA.

2. **Consent and FERPA Exemptions.** LEA acknowledges that certain information shared with or obtained by Provider pursuant to this DPA, may be considered an education record under FERPA. LEA specifically represents, warrants, and covenants to Provider that it has and will:
   (a) Comply with the School Official Exemption, as set forth in 34 C.F.R. 99.31 (a)(1)(i)(B), including, without limitation that its annual notice under FERPA includes vendors, such as the Provider, as "School Officials" and defines "legitimate educational interest" to include services such as the type provided by Provider;

3. **Reliance by Provider**. LEA acknowledges that Provider depends on LEA to provide accurate information regarding the Student Data and agrees to correctly tag all artwork and Pupil Generated Content corresponding to whether or not it contains personally identifiable information before it is published and provided to Provider. LEA further acknowledges that Provider also depends on LEA to ensure LEA's compliance with applicable state and federal law, including FERPA, regarding the disclosure of any Student Data that will be shared with Provider.

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

5. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or

suspected unauthorized 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 access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all Massachusetts and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, 603 C.M.R. 23.00 and Massachusetts General Law, Chapter 71, Sections 34D to 34H.

2. **Authorized Use**. Student Data shared pursuant to this DPA, including persistent unique identifiers, shall be used for no purpose other than is permitted by this DPA, including Exhibit A, and as authorized under the statutes referred to in subsection (1), above. Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, any student data, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, except as contemplated in this DPA, including Exhibit A, or as authorized by a parent or legal guardian in writing, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

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 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. **De-Identified Data**. De-identified information, as defined in Exhibit "C", 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, as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b), and shall survive termination of this DPA. Provider agrees not to transfer de-identified Student Data, except for student artwork with additional parental consent, to any party unless that party agrees in writing not to attempt re-identification., and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Except as is already contemplated and agreed to in this DPA, prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

5. **Disposition of Data**. Provider shall dispose or delete all personally identifiable data obtained under the DPA when it is no longer needed for the purpose for which it was obtained and, upon written request from the LEA, shall transfer said data to LEA or LEA's designee within sixty (60) days of the written request from the LEA and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition or requires Provider to dispose of personally identifiable data obtained directly from the individual, or that is part of a separate account established and maintained by a student, parent or legal guardian of a student. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal

information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Student Data" FORM, A Copy of which is attached hereto as Exhibit "D").

6. **Advertising Prohibition**. Provider is prohibited from leasing, renting, using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising or other commercial efforts by a Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service as described in Exhibit A to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Services as described in Exhibit A.. This Advertising Prohibition does not prohibit the Provider from obtaining additional consent directly from a parent / legal guardian to use Student Data when promoting custom products as part of its mission to perform school fundraisers as described in Exhibit A. The Provider will NOT use parent contact information provided by LEA except to obtain permission to display artwork and to invite parents to create a separate account.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized access, disclosure, use or acquisition by an unauthorized person. The general security duties of Provider are set forth below. These measures shall include, but are not limited to:

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

    b. **Destruction of Data**. As set forth in more detail in Article IV, Paragraph 5, Provider shall destroy or delete all Personally Identifiable Data contained in Student Data and obtained under the DPA when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Subject to the exceptions stated in Article IV, Paragraph 5, nothing in the DPA authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

    c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the DPA in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the DPA, except as necessary

to fulfill the purpose of data requests by LEA or as otherwise set forth in this DPA. The foregoing does not limit the ability of the Provider to allow any necessary Subprocessors to view or access data as set forth in Article IV, section 4.

d. Employee Training. The Provider shall provide recurring, periodic (no less than annual, with additional sessions as needed throughout the year to address relevant issues/changes, such as (but not necessarily limited to) new or evolving security threats, changes to security protocols or practices, changes to software and/or hardware, identified vulnerabilities, etc.) security training to those of its employees who operate or have access to the system. Such trainings must be tailored to the Provider's business and cover, but not necessarily be limited to, the following topics: common types of attackers (e.g., cyber criminals, hacktivists, government sponsored groups, inside threats, etc.); common types of attacks (e.g., social engineering, spoofing, phishing, etc.) and how the information sought is typically used; identifying threats, avoiding threats, physical security and environmental controls; internal policies and procedures; and safe internet habits. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

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

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

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

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

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

j. Audits. Upon written request, not to exceed one request per year, except in the case of a verified breach, in which case the limitation would not apply, the Provider will allow the LEA to audit the security and privacy measures outlined in this DPA to ensure protection of the Student Record or any portion thereof, subject to reasonable time and manner restrictions. The Provider will cooperate reasonably with the LEA and any state or federal agency with oversight authority/jurisdiction in connection with any such audit and shall

provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the delivery of Services to the LEA.

2. **Data Breach**. In the event that Provider becomes aware of an unauthorized acquisition of Student Data, an "Incident", Provider shall provide notification to LEA within thirty (30) days of the Provider becoming aware of the Incident. Provider shall follow the following process:
    - **a.** The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "When it Occurred," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
    - **b.** The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
        - **i.** The name and contact information of the reporting LEA subject to this section.
        - **ii.** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
        - **iii.** If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
        - **iv.** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
        - **v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
        - **vi.** The estimated number of students and teachers affected by the breach, if any.
    - **c.** At LEA's discretion, the security breach notification may also include any of the following:
        - **i.** Information about what the Provider has done to protect individuals whose information has been breached.
        - **ii.** Advice on steps that the person whose information has been breached may take to protect himself or herself.
    - **d.** Provider agrees to adhere to all requirements in the Massachusetts Data Breach law and in federal law with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
    - **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 data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a copy of said written incident response plan.
    - **f.** At the request and with the assistance of the LEA, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent and as long as any service agreement or terms of service, to the extent one exists, has lapsed or has been terminated. The LEA may terminate this DPA with the Provider if the Provider breaches any terms of this DPA.

3. **Effect of Termination Survival**. If the DPA is terminated, the Provider shall dispose of LEA's data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA, inclusive of its exhibits, shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA, IDEA. COPPA, PPRA, 603 CMR 28.00, 603 C.M.R. 23.00, and Massachusetts General Law, Chapter 71, Sections 34D to 34H. In the event there is conflict between the terms of the DPA and any other agreement between the LEA and Provider, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of any other agreement shall remain in effect.

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

   James Meyers
   CEO | Artsonia LLC
   1350 Tri-State Parkway, Ste. 106, Gurnee, IL 60031
   (224) 538-5040 | meyers@artsonia.com

   The designated representative for the LEA for this Agreement is:

   Leisha Simon
   Director of Technology
   41 Cochituate Road, Wayland, MA 01778
   508.358.3714
   leisha_simon@wayland.k12.ma.us

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

shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

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

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

9. **Authority.** Provider represents that it has taken reasonable steps to ensure that its related or associated entities, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way will protect Student Data in manner consistent with the terms of this DPA.

10. **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.

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 Massachusetts 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 my 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.

    Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation

at any time of their electronic signature for any other reason in writing.

If either party would like a paper copy of this Agreement, they may request a copy from the other party.

12. **Multiple Counterparts:** This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart.

ARTICLE VII- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this to any other school district who signs the acceptance in said Exhibit.

[*Signature Page Follows*]

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

WAYLAND PUBLIC SCHOOLS

By: Arthur Unobskey Date: August 20, 2020
Arthur Unobskey (Aug 20, 2020 17:48 EDT)

Printed Name: _____ Arthur Unobskey _____ Title/Position: ____ Superintendent of Schools

ARTSONIA LLC

By: James Meyers Date: 8/18/2020
James Meyers (Aug 18, 2020 13:51 CDT)

Printed Name: James Meyers Title/Position: CEO

EXHIBIT "A"

DESCRIPTION OF SERVICES

Artsonia is the world's largest online student art museum, offering a free, educational resource to schools, teachers and parents. Art teachers publish student artwork to the school's online gallery, creating a digital portfolio for each individual student. This enables teachers to explain what the student has learned and what methods were used in the creative process. Teachers also help get the parent connected to the student portfolios, which enable the parents to unlock additional features of Artsonia.

Parents may decide to allow Artsonia to display their child's artwork in the school's public online-gallery for other family members, friends, and art appreciators to enjoy. Parents may also upload artwork created outside of school to the student's portfolio. Artsonia doesn't display artwork to the public unless it has parental consent and a teacher or parent has verified that the artwork does not contain personally identifiable information. Parents know and agree that their child's publicly available artwork will be associated with the student's school and a unique screenname generated by Artsonia. If the teacher or parent determines that there is personal information and does not mask or remove it, then the artwork should not be made publicly available. Instead, it should only be viewed by teachers at the student's school, the student's parents, and fan club members the parent has authorized for the student.

Parents, family members, friends, and other art appreciators may purchase keepsakes from our gift shop with a student's publicly available artwork on the item. Parents and parent authorized fan club members are also able to purchase keepsakes with their child's private artwork as well. Twenty percent (20%) of all purchases are donated back to the school's art program. Parents and students also have the opportunity to participate in additional activities, including special exhibits, art contests and other art-related events.

Artsonia notifies the parents, family members and friends of the student-artists when new artwork is available and invite them to browse the school gallery. We also let our users know about other aspects of our service, such as our gift shop, sales, products, shipping information, website features, events, updates, contests, exhibits, and general information about Artsonia.

On Artsonia, participating art teachers also have the opportunity to share project ideas, post and view lesson plans, participate in art contests and events, and make other community-based connections with fellow art teachers.

EXHIBIT B

SCHEDULE OF DATA

Category of Data	Elements	Used by Provider
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	Yes, for authentication and to help with general navigation of the website.
	Other application technology meta data - Please specify:	No.
Application Use Statistics	Meta data on user interaction with application	We store machine/device type and operating system usage for debugging and customer support, as well as aggregate data.
Assessment	Standardized test scores	No.
	Observation data	No.
	Other assessment data - Please specify:	Teachers sometimes use the student artwork portfolios as an assessment tool.
Attendance	Student school (daily) attendance data	No.
	Student class attendance data	No.
Communications	Online communications that are captured (emails, blog entries)	Visitors over 13 can leave comments for students or compliments for teachers. Students can leave comments using the class portal with teacher supervision. Teachers can create announcements for students, as well as videos instructing students for projects. Teachers can leave feedback for students and parents.
Conduct	Conduct or behavioral data	No.
Demographics	Date of Birth	No. But for COPPA related purposes, we ask for birth year to ensure users of certain features are over 13. We do not store this information.
	Place of Birth	No.
	Gender	No.
	Ethnicity or race	No.
	Language information (native, preferred or primary language spoken by student)	No. But some sections are also translated to Spanish, and if you select the Spanish version, that preference is stored in a cookie for improved service.
	Other demographic information - Please specify:	No.
Enrollment	Student school enrollment	No.
	Student grade level	Yes, to help teachers organize their roster when submitting student artwork and for display purposes on public artwork.
	Homeroom	Yes, to help teachers organize their roster when submitting student artwork.
	Guidance counselor	No.
	Specific curriculum programs	No.
	Year of graduation	No.

	Other enrollment information - Please specify:	No.
Parent/Guardian Contact Information	Address	No, unless they purchase a keepsake with their child's artwork.
	Email	Yes, supplied by the child's teacher, by the student within their class portal, by the parent directly after receiving a code from the teacher, or by another parent when adding an additional parent to a child account
	Phone	Yes, supplied by the parent when registering for an account, or when creating another account for a spouse.
Parent/Guardian ID	Parent ID number (created to link parents to students)	Yes, usually the parent's email address provided by the teacher parent, or by the student within the class portal. We also provide a parent code that the parent uses for registration.
Parent/Guardian Name	First and/or Last	Yes.
Schedule	Student scheduled courses	No.
	Teacher names	Yes. Only the art teacher's name that is administering the student art gallery.
Special Indicator	English language learner information	No.
	Low income status	No.
	Medical alerts	No.
	Student disability information	No.
	Specialized education services (IEP or 504)	No.
	Living situations (homeless/foster care)	No.
	Other indicator information - Please specify:	No.
Student Contact Information	Address	No.
	Email	No.
	Phone	No.
Student Identifiers	Local (School district) ID number	Yes. The school name is collected from the teacher upon registration.
	State ID number	No.
	Vendor/App assigned student ID number	Yes, each student receives a unique screenname.
	Student app username	No, but schools are given a class portal code for students to then login to their school to submit student artwork.
	Student app passwords	Yes, if the teacher has enabled student PINs when students are submitting their student artwork.
Student Name	First and/or Last	Yes.

Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	No.
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	No, unless the teacher creates an art gallery featuring a certain extracurricular group and the artwork is published within that group (eg an after-school art club).
Student Survey Responses	Student responses to surveys or questionnaires	No.
Student work	Student generated content; writing, pictures etc.	Yes, artwork created in art room, which could also contain photographs, videos, art titles, artist statements and other material the student created.
	Other student work data - Please specify:	See above.
Transcript	Student course grades	No, unless teacher writes in grades in feedback for artwork.
	Student course data	No.
	Student course grades/performance scores	No, unless teacher writes in grades in feedback for artwork.
	Other transcript data - Please specify:	Teachers can submit feedback on artwork, which can be shared with the student's parent/guardian. Depending on the feedback, this could be considered part of a student transcript.
Transportation	Student bus assignment	No.
	Student pick up and/or drop off location	No.
	Student bus card ID number	No.
	Other transportation data - Please specify:	No.
Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT "C"

DEFINITIONS

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them. The Provider's specific steps to de-identify the data will depend on the circumstances, but should be appropriate to protect students. Some potential disclosure limitation methods are blurring, masking, and perturbation. De-identification should ensure that any information when put together cannot indirectly identify the student, not only from the viewpoint of the public, but also from the vantage of those who are familiar with the individual.

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

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" means information 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. PII may include, but is not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, unless this information has been de-identified or anonymized. De-Identified Information is not PII. PII may include, without limitation, the following:

First Name	Home Address
Last Name	Subject
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
	Search Activity
Photos	Voice Recordings
Videos	Date of Birth
Grade	Classes
Place of birth	Social Media Address

Credit card account number, insurance account number, and financial services account number

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, artwork, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications when use of such instructional software or applications were assigned to the pupil by a teacher or other local educational LEA employee and which is, therefore, maintained by the Provider as a School Official.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (a)(1)(i)(B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians using accounts associated with or at the direction of the LEA, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, the name of the student's parents or other family members, place of birth, social media address, unique pupil identifier, and credit card account number, insurance account number, and financial services account number, student identifiers, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of Massachusetts and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute and does not include that information that has been anonymized or de-identified, including De-Identified Data, or anonymous usage data regarding a student's use of Provider's services.

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

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor" and is referred to as "Service Provider" or "Third Party Service Provider" in Artsonia's Terms of Service and Privacy Policy) means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software or Services, and who has access to PII.

Targeted Advertising: Targeted Advertising means presenting an advertisement or marketing to a student on the Provider's site, service, or application, or on any other site, service, or application where the selection of the advertisement or marketing is based on Student Data or inferred from the student's

online behavior or usage of the Provider's website, online service or mobile application by such student. Targeted Advertising includes advertising to a student at an online location based upon a single search query without collection and retention of a student's online activities over time. Targeted Advertising includes targeted advertising that is based upon factors, including, but not limited to, the student's recent browsing history, the student's language and the student's location. Targeted Advertising does not include advertising to a student at an online location based upon that student's current visit to that location.

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

LEA directs Artsonia LLC to dispose of 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 data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

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

2. Nature of Disposition

___ Disposition shall be by destruction or deletion of data.

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

[Insert or attach special instructions.]

3. Timing of Disposition

Data shall be disposed of by the following date:

____ As soon as commercially practicable

_____By (Insert Date]

4. Signature

_____
(Authorized Representative of LEA

_____
Date

5. Verification of Disposition of Data

_____ _____
Authorized Representative of Provider Date