

STUDENT DATA PRIVACY AGREEMENT

(NDPA Vendor Modified Version AS2021a)

and

ARTSONIA

This Student Data Privacy Agreement (“DPA”) is entered into on the date of full execution (the “Effective Date”) and is entered into by and between _____, located at _____ (the “Local Education Agency” or “LEA”) and Artsonia LLC, located at 1350 Tri-State Parkway, Suite 106, Gurnee, IL 60031 (the “Provider” or “Artsonia”).

RECITALS

WHEREAS, the Provider is providing educational or digital services to LEA;

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. § 1232g (34 CFR Part 99), the Children’s Online Privacy Protection Act (“COPPA”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations; and,

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

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

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions—Check if Required.**
 - If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 - If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H"**
 - If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms.
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire three years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “Services”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: James Meyers

Title: CEO, Artsonia LLC

Address: 1350 Tri-State Parkway, Suite 106, Gurnee, IL 60031

Phone: (224) 538-5040

Email: meyers@artsonia.com

The designated representative for the LEA for this DPA is:

Name:

Title

Address:

Phone:

Email:

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

LEA:

By:

Date:

Printed Name:

Title/Position:

Artsonia LLC

By:

Date:

Printed Name: James Meyers

Title/Position: CEO, Artsonia, LLC

STANDARD CLAUSES

Version 3.0

ARTICLE I: PURPOSE AND SCOPE

- Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities of the Parties to protect Student Data transmitted to pursuant to the Services, including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services for the 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, with respect to its use of Student Data obtained through the Services it provides to the LEA.
- Student Data to Be Provided.** In order to perform the Services, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
- DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies, and other related documents.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

- Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions of any portion thereof, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data pursuant to the Services, notwithstanding the above.
- Parent Access.** To the extent required by law, the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Educational Records and/or Student Data, correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA’s request for Student Data in a student’s records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or

individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If Student Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.
4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to in this DPA.

3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation user content or other non-public information and/or personally identifiable information contained in the Student Data other than as otherwise directed or permitted by the LEA and/or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Except as otherwise permitted by the Service Agreement and this DPA, Provider will not sell Student Data to any third party.
5. **De-Identified Data.** Unless otherwise permitted by the DPA, including Exhibit A, Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA, and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors and as otherwise permitted by the DPA, including Exhibit A, Provider agrees not to transfer deidentified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Unless otherwise permitted by the DPA, including Exhibit A, prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data obtained under the Service Agreement after providing the LEA with reasonable prior notice. This duty to dispose of Student Data shall not extend to Student Data that had been De-Identified; Student Data placed in a separate student account pursuant to section II, 3; or information that is not Student Data or is not part of the Service Agreement because it is part of a separate account maintained by a student, parent or legal guardian. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D."

- 7. Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Services to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); (ii) to make product recommendations to teachers or LEA employees; or, (iii) to notify account holders about new educational product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

- 1. Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
- 2. Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of Services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any such audit or investigation and shall provide reasonable access to the Provider's facilities, staff, agents LEA's Student Data, and all records pertaining to the LEA and the Provider's delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.
- 3. Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
- 4. Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider, the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

- a.** The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i.** The name and contact information of the reporting LEA subject to this section;
 - ii.** A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;
 - iii.** The date of the notice and, if it 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;
 - iv.** Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and,
 - v.** A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- b.** Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- c.** Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- d.** LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- e.** In the event of a breach originating from LEA's use of the Services, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of “General Offer of Privacy Terms” (General Offer, attached hereto as **Exhibit “E”**), be bound by the terms of **Exhibit “E”** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

- 1. Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any Service Agreement or contract if the other party breaches any terms of this DPA.
- 2. Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA’s Student Data pursuant to Article IV, Section 6.
- 3. Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
- 4. Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
- 5. Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

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

7. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT “A”
DESCRIPTION OF SERVICES

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 an online gallery, creating a digital portfolio for each individual student that Artsonia maintains in a virtual archive. 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 also decide to allow Artsonia to display their child’s artwork in Artsonia’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 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 invites 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 Metadata	IP addresses of users, use of cookies, etc.	Yes, for authentication and to help with general navigation of the website.
	Other application technology Metadata - please specify	No.
Application Use Statistics	Metadata 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 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 thirteen can leave comments for students or compliments for teachers. Students can leave comments using the class portal with teacher supervision. Teachers can create announcements and instruction videos for students and 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 thirteen. 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. If a user selects the Spanish version, that preference is stored in a cookie for improved service.

	Other demographic information - please specify	No.
Enrollment	Student school enrollment	Yes, students are linked to their existing school for teachers and students to submit artwork.
	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, which was provided by the teacher, parent, or 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 (e.g., 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	See above.

	specify	
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	Flag for artwork containing PII	Teachers designate whether or not artwork contains PII. This is used to help determine whether or not artwork can be available to the public.

EXHIBIT “C” DEFINITIONS

De-Identified Data and De-Identification. Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to any information that alone or in combination is linkable to a specific student and provided that the educational agency or other party has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

Educational Records. The term “Educational Records” means records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata. “Metadata” is information that provides meaning and context to other data being collected, including but not limited to date, time, and purpose of creation. Metadata that has been stripped of all direct and indirect identifiers is not considered personally identifiable information.

Operator. The operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “Operator” for the purposes of this section.

Originating LEA. An “Originating LEA” is an LEA who originally executes the DPA in its entirety with the Provider.

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 Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Student Generated Content. The term “student-generated content” means materials or content created by a student in the Services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official. For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that (1) performs an institutional service or function for which the agency or institution would otherwise use employees; (2) is under the direct control of the agency or institution with respect to the use

and maintenance of Student Data including Educational Records; and, (3) Is subject to 34 CFR § 99.33(a) governing the use and redisclosure of personally identifiable information from Educational Records.

Service Agreement. The “Service Agreement” refers to the Contract, Purchase Order, and Terms of Service or Terms of Use.

Student Data. Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students’ parents/guardians on behalf of the LEA or in connection with an account designated by 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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents’ names, or any other information or identification number that would provide information about a specific student. Student Data includes Metadata. Student Data further includes “personally identifiable information” (or “PII”), as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Educational Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit “B”** is confirmed to be collected or processed by the Provider pursuant to the Services where such data is provided by or on behalf of the LEA. Student Data shall not constitute and does not include: (a) information that has been gathered or transmitted to Provider directly by the student, parent, legal guardian, or other third party that was not directed by the LEA; (b) information obtained outside of the Service Agreement; and, (c) information that has been anonymized or de-identified, or anonymous usage data regarding a student’s use of Provider’s services.

Subprocessor. For the purposes of this DPA, the term “Subprocessor” (sometimes referred to as the “Subcontractor” in this Agreement or “Service Provider” and “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 otherwise operate and/or improve its service, and who has access to Student Data.

Subscribing LEA. A “Subscribing LEA” is an LEA that was not party to the original Service Agreement and who accepts the Provider’s General Offer of Privacy Terms.

Targeted Advertising. “Targeted Advertising” means presenting an advertisement to a student where the selection of the advertisement is based on Student Data, inferred over time from the usage of the Operator’s website, online service, or mobile application by that student, or the retention of that student’s online activities or requests over time for the purpose of targeting subsequent advertisements. “Targeted advertising” does not include any advertising to a student on a website based on the content of the web page or in response to a student’s response or request for information or feedback.

Third Party. The term “Third Party” means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Educational Records

and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term “Third Party” when used to indicate the provider of digital educational software or services is replaced by the term “Provider.”

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement 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. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By [Insert Date]

4. Signature

By: _____
Authorized Representative of LEA

Date: _____

5. Verification of Disposition of Data

By: _____
Authorized Representative of Artsonia LLC

Date: _____

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and the LEA to any other school district ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the originating Service Agreement; or, three (3) years after the date of Provider's signature to this Form. **ARTSONIA LLC**

Printed Name: James Meyers Title/Position: CEO

By: _____ Date: _____

Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address: Meyers@Artsonia.com

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the LEA and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5.****

[INSERT NAME OF SUBSCRIBING LEA]

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

School District Name: _____

County of LEA: _____



Designated Representative of the LEA

Name

Title

Address

Telephone

Email

EXHIBIT “F”
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange (“Edspex”) works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* (“Cybersecurity Frameworks”) that may be utilized by Provider.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology (“NIST”)	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology (NIST”)	NIST SP800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization (“ISO”)	Information technology – Security techniques – Information security management systems (ISO 2700 series)
	Secure Control Framework Council, LLC	Security Control Framework (SCF)
	Center for Internet Security (“CIS”)	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (“OUSD(A&S”)	Cybersecurity Maturity Model Certification (CMMC, FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here.

EXHIBIT “G” – Supplemental SDPC State Terms for []

Version ____AS2021a_____

[The State Supplement is an *optional* set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit “H”** in this proposed structure).]

EXHIBIT “H” – Additional Terms or Modifications

Version __2021a_____

LEA and Provider agree to the following additional terms and modifications:

- 1. Reliance by Provider.** LEA acknowledges that Provider depends on LEA to provide accurate information regarding Student Data and agrees to correctly tag all artwork and Student 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.
- 2. Consent to Electronic Signature, Counterparts.** This Agreement may be executed and delivered by electronic signature and in two or more counterparts, each of which will be deemed an original, but all of which together will constitute one and the same instrument. The LEA(s) (including the Originating LEA and any Subscribing LEA(s)) and Provider agree and consent that delivery and execution of this Agreement and any modifications or amendments thereto may be accomplished electronically and that electronic signatures (within the meaning of the Electronic Signatures in Global and National Commerce Act) to this Agreement by their respective signatories are intended to authenticate such signatures and to give rise to a valid, enforceable, and fully effective Agreement.
- 3. Exhibits Incorporated by Reference, Priority.** This DPA incorporates all exhibits hereto by reference in their entirety. In the event of a conflict between either Exhibit A or Exhibit H and the SDPC Standard Clauses and/or the Supplemental State Terms, Exhibit A and Exhibit H will control. Exhibits A and H shall control over all other provisions and/or terms in the DPA, Service Agreement, and any other documents, including exhibits thereto.
- 4. Data Obtained Directly from Students, Parents, Third Parties.** Student Data limited to information gathered by or transferred to the Provider by or on behalf of the LEA, including using accounts designated by or at the direction of the LEA. Information obtained directly from a student, parent, legal guardian, or any other party who is not acting on behalf of the LEA, or information that is otherwise transmitted to Provider outside of the Service Agreement, is not Student Data and is not subject to the DPA.