

Student Data Privacy Addendum / Data Processing Agreement — Nationwide Draft

Theatre4u · ArtsTracker · DRAFT for attorney review · August 2026 Artstracker LLC ·
10441 Stanford Ave. #1155, Garden Grove, CA 92842 · hello@theatre4u.org

1. Parties and purpose

This Student Data Privacy Addendum and Data Processing Agreement ('Addendum') is entered into by Artstracker LLC ('Provider'), owner of the Theatre4u and ArtsTracker services (the 'Service'), and the subscribing school or district ('LEA'), which may be located in any state. It supplements the Provider's Terms of Service and governs the handling of Student Data and other personal information the LEA makes available through the Service. If it conflicts with the Terms, this Addendum controls for Student Data and Pupil Records.

2. Definitions

- 'Student Data' means information that identifies a currently or formerly enrolled student and is provided to or collected by the Service on the LEA's behalf, consistent with FERPA education records, California 'covered information' (Bus. & Prof. Code §22584), and the equivalent category under the LEA's applicable state student privacy law. Student Data includes pupil-generated content.
- 'Pupil Records' has the meaning in California Education Code §49073.1, or the equivalent category of protected student records under the LEA's state law.
- 'De-Identified Data' means data with all direct and indirect identifiers removed such that a student cannot reasonably be re-identified.
- 'Service Provider / Operator' describe Provider's role under FERPA and SOPIPA, and under comparable state student privacy laws, respectively.

3. Roles, ownership, and control

- The LEA is the owner of and controls all Pupil Records and Student Data. Provider acts as a service provider processing on the LEA's behalf and, where applicable, as a 'school official' with a legitimate educational interest under FERPA, under the LEA's direct control.
- Pupil Records continue to be the property of and under the control of the LEA (Ed. Code §49073.1(b)(1), or the equivalent under the LEA's state law). The LEA may access, export, correct, or delete Student Data at any time. Provider will assist the LEA with a pupil's transfer of pupil-generated content where the Service supports it.
- Provider will use Student Data only to provide and support the Service for the LEA, and for no other purpose.

4. Prohibited uses (SOPIPA aligned and comparable state laws)

Provider will NOT: sell Student Data; use or disclose Student Data for targeted advertising; create a profile of a student except in furtherance of school purposes; or use Student Data

for any commercial purpose. Provider will not use Student Data to train artificial intelligence models, will not disclose Student Data except as this Addendum permits, and will not use persistent identifiers to build a profile of a student except for school purposes. Advertising measurement tools (Google Analytics, Meta Pixel) run only on Provider's public marketing pages and never receive Student Data or LEA content. These commitments are made under SOPIPA and comparable student privacy laws in other states.

5. Permitted disclosures and subprocessors

- Provider uses the subprocessors listed in Exhibit A solely to provide the Service. Provider will bind subprocessors to obligations no less protective than this Addendum and will give the LEA at least 30 days advance notice of a material change to the subprocessor list. If the LEA reasonably objects to a new subprocessor, the LEA may terminate the affected subscription and receive a pro rata refund of prepaid fees.
- Provider will not otherwise disclose Student Data except as directed by the LEA or as required by law, in which case Provider will, unless prohibited, notify the LEA.

6. Security

Provider maintains administrative, physical, and technical safeguards including: encryption in transit (TLS 1.2+) and at rest (AES-256); Row-Level Security isolating each organization's data; hashed credentials; least privilege administrative access; and security headers. Provider's infrastructure providers maintain SOC 2 Type II (Supabase) and can supply attestations on request. Provider limits access to Student Data to personnel who need it to provide the Service, trains those personnel on data privacy and security obligations, and reviews administrative access periodically.

7. Security incidents and breach notification

Provider will notify the LEA without undue delay and no later than seventy-two (72) hours after confirming a security incident affecting the LEA's Student Data, will cooperate with the LEA's investigation and notification obligations, and will describe the incident, data involved, and remediation. Provider will support the LEA in providing any notice to affected parents and pupils required by California Education Code §49073.1 and by the LEA's applicable state breach notification law.

8. Parent and pupil rights

Provider will assist the LEA in enabling parents, guardians, and eligible pupils to review, correct, and request deletion of the student's personally identifiable information, consistent with FERPA, California Education Code §49073.1, and the LEA's applicable state law. Requests are directed to the LEA; Provider supports the LEA's response.

9. Return and deletion

On termination or LEA request, Provider will return and/or delete Student Data within thirty (30) days and certify deletion, except for De-Identified Data and backup copies retained for a limited period before routine deletion. Backup copies are deleted in the

ordinary backup cycle described in the Privacy Policy. Provider will not retain Student Data beyond the period necessary to provide the Service (Ed. Code §49073.1 and applicable state law).

10. De-identified data

Provider may use De-Identified Data only to operate, maintain, and improve the Service, and will not attempt to re-identify it or share it in a manner that could reasonably identify a student.

11. Compliance, audit, and cooperation

Provider will comply with FERPA, COPPA (for students under 13, relying on school authorization for school authorized educational use only), PPRA, SOPIPA, and applicable state student data privacy laws, and will reasonably cooperate with the LEA's security reviews and questionnaires. Provider will supply available third-party attestations for its infrastructure providers on request. On-site audits are not included.

12. Term, order of precedence, governing law

This Addendum is effective on the LEA's subscription start and continues while the LEA uses the Service. Order of precedence for pupil records: if the parties execute the SDPC National Data Privacy Agreement or the LEA's own data privacy agreement, that agreement and its state exhibit govern; otherwise this Addendum, then the LEA's order form, then the Terms of Service. Governing law: for an LEA located in California, California law governs; for an LEA located in another state, the law of the LEA's state governs this Addendum, and any state specific requirements are set by the applicable state exhibit in Exhibit C. Disputes between Provider and an LEA proceed in a court of competent jurisdiction. The consumer arbitration and class action waiver provisions in the Terms of Service do not apply to an LEA or other public entity.

Exhibit A — Subprocessors

Provider	Purpose	Location / notes
Supabase	Database, auth, storage	AWS us-east-1; SOC 2 Type II
Amazon Web Services	Cloud hosting	us-east-1
Vercel	Web hosting / CDN	Serves web requests; keeps standard server and CDN logs (IP address, request metadata); no content stored
Resend	Email delivery	Recipient email only
Stripe	Payment processing	No student data; stores card data directly
Anthropic	In-app Help assistant (help chat text only)	US; SOC 2 Type II
Google	Web fonts; optional Google Drive photo import when a	US / global

user chooses it

Exhibit B — Description of processing

- Nature and purpose: cloud inventory, resource sharing, and program administration for arts programs.
- Categories of data subjects: staff and administrators; incidentally, students added as team members or appearing in uploaded photos.
- Categories of Student Data: name and school email address of a student team member; images or records that staff upload, which may include a student's likeness; and pupil-generated content where the LEA enables it.
- Duration: term of the LEA's subscription plus the defined deletion window.

Exhibit C — State specific requirements

For an LEA outside California, attach the LEA's state exhibit or the Student Data Privacy Consortium (SDPC) National Data Privacy Agreement state exhibit for the LEA's state. For a California LEA, attach the California CSDPA exhibit.