FERPA Data Privacy Addendum

Between: **Its One App, LLC (d/b/a Its1Ticket)** ("Provider"), and the educational agency or institution identified in the signature block ("LEA" — Local Educational Agency).
This FERPA Data Privacy Addendum (the "Addendum") supplements and is incorporated into the Terms of Service between Provider and LEA (the "Agreement"). If there is a conflict between this Addendum and the Agreement with respect to Student Data, this Addendum controls.

1. Purpose & Background

The LEA uses the Provider's ticketing, box-office, and event-registration platform (the "Service"). In providing the Service, the Provider may receive or create records that are directly related to students and maintained by or on behalf of the LEA ("Student Data", as further defined below). This Addendum sets the terms under which the Provider handles Student Data in compliance with the Family Educational Rights and Privacy Act ("FERPA", 20 U.S.C. § 1232g; 34 C.F.R. Part 99) and applicable state student-privacy laws.

2. Definitions

- **Education Records / Student Data:** records, files, documents, and other materials that contain information directly related to a student and are maintained by the LEA or by the Provider acting for the LEA, including registration responses, rosters, dates of birth, grade level, guardian and emergency contact information, health/medical notes, and any student photo captured for ticket verification. "Eligible Student" means a student who has reached 18 years of age or is attending a postsecondary institution.
- **De-Identified Data:** data from which all personally identifiable information has been removed such that a student cannot reasonably be identified, directly or indirectly.
- **School Official:** a party to whom the LEA has outsourced an institutional service or function under 34 C.F.R. § 99.31(a)(1)(i)(B).
- **Subprocessor:** a third party engaged by the Provider to process Student Data in furtherance of the Service (see Exhibit B).

3. Designation as a "School Official"

The LEA designates the Provider as a "School Official" with a "legitimate educational interest" in the Student Data, performing an institutional service or function for which the LEA would otherwise use its own employees, under the FERPA school-official exception (34 C.F.R. § 99.31(a)(1)(i)(B)). The Provider:

- performs an institutional service or function for the LEA;
- is under the direct control of the LEA with respect to the use and maintenance of Student Data;
- uses Student Data only for the authorized purpose of providing the Service; and

- does not re-disclose Student Data except as permitted by this Addendum and FERPA.

4. Ownership & Control of Student Data

Student Data is and remains the property of the LEA. The Provider obtains no rights in Student Data other than the limited right to process it to provide the Service. The LEA controls what Student Data is collected (including the content of any custom registration fields) and may access, export, correct, or request deletion of Student Data at any time through the Service or by written request.
The LEA retains sole discretion over the content and collection of any custom registration fields and over whether to enable photo-based ticket verification. Any Student Data collected through such features remains subject to this Addendum.

5. Permitted Use; Prohibited Uses

- **Permitted:** The Provider will use Student Data solely to operate, maintain, support, and improve the Service as provided to the LEA (including using De-Identified Data derived from Student Data to improve the underlying platform technology and features generally, consistent with Section 12).
- **Prohibited:** The Provider will not:
- sell, rent, or trade Student Data;
- use or disclose Student Data for advertising, marketing, or to create targeted advertising or a commercial profile of a student or the LEA;
- use Student Data to train third-party or general-purpose AI/ML models;
- re-disclose Student Data to any third party, except to Subprocessors under Section 8 or as compelled by law under Section 11.

6. Parental / Eligible-Student Rights

The LEA remains responsible for FERPA notices, consent, and any designation of "directory information." The Provider will support the LEA in fulfilling parents'/eligible students' rights to inspect, review, request correction or deletion (where required or permitted by FERPA, applicable state law, or LEA policy) of Student Data by providing the LEA reasonable access and export tooling. The Provider will refer any rights request it receives directly to the LEA.

7. Data Security

The Provider maintains administrative, physical, and technical safeguards appropriate to the sensitivity of Student Data, including:

- encryption of Student Data in transit using TLS 1.2 or higher and encryption at rest using AES-256 (or equivalent industry-standard encryption) for all stored Student Data, including but not limited to student photos;
- row-level security and role-based access controls restricting Student Data to authorized

LEA administrators and Provider personnel with a need to know;
- an append-only access/disclosure log recording access to rosters, registration responses, and student photos, available to the LEA;
- marking and audit tracking of designated sensitive fields (e.g., medical notes), including visual indicators in the administrative interface and flagging in the access/disclosure log when sensitive data is viewed or accessed;
- least-privilege access, secure credential management, and logging/monitoring.

As the organization scales, the Provider intends to pursue independent third-party security assessments, which may include a SOC 2 examination and penetration testing. Upon request, the Provider will provide the LEA with a written summary of its current security controls, recent security improvements, and its planned assessment roadmap. The Provider maintains a documented incident-response plan that addresses Student Data incidents and includes the notification procedures in Section 9.

8. Subprocessors

The Provider may engage the Subprocessors listed in Exhibit B to process Student Data. Each Subprocessor is bound by written terms requiring data-protection obligations no less protective than this Addendum and use of Student Data only to provide services to the Provider. The Provider remains responsible for its Subprocessors' performance.

The current list of Subprocessors is set forth in Exhibit B and is available upon request or via the Service administrative portal. Provider will provide written notice to the LEA (via email to the LEA's designated privacy or administrative contact and/or through the Service administrative interface) of any intended addition, removal, or material change to a Subprocessor that will process Student Data, at least thirty (30) days before the change takes effect. The LEA may object in writing within fifteen (15) days of notice if it reasonably believes the new or changed Subprocessor does not provide adequate data-protection safeguards. In the event of a timely objection, the parties will negotiate in good faith. If the concern is not resolved within fifteen (15) days, the LEA may terminate the Agreement or the affected portion of the Service without penalty, and Provider will reasonably assist with an orderly transition of data.

Provider has entered into (and will maintain) written agreements with each Subprocessor that include data-protection obligations no less protective than this Addendum, including appropriate flow-down of FERPA obligations, security requirements, breach-notification timelines to Provider, restrictions on further subprocessing, and return/deletion rights. Provider remains responsible for ensuring its Subprocessors comply with the obligations set forth in this Addendum and will take commercially reasonable steps to address any Subprocessor non-compliance, including, where appropriate, terminating or replacing non-compliant Subprocessors. Provider shall be liable for damages arising from a Subprocessor's breach of this Addendum to the same extent Provider would be liable had it committed the breach itself, subject to the aggregate liability limitations in Section 13.

9. Data Breach Notification

Upon confirming an unauthorized acquisition, access, use, or disclosure of Student Data, the Provider will notify the LEA in writing without unreasonable delay and in no event later than

forty-eight (48) hours after such confirmation, or such shorter period as required by applicable state or federal law (whichever is earlier). The initial notice will be followed by a detailed written report describing: (i) the nature of the incident; (ii) the categories of Student Data involved; (iii) the approximate number of affected students and/or records (if known); (iv) likely consequences; (v) measures taken or proposed to address the incident and mitigate potential harm; and (vi) contact information for follow-up. Provider will cooperate fully and promptly with the LEA's investigation, internal response, required notifications to parents/eligible students/regulators, and remediation efforts. Provider will not notify affected individuals or issue public statements about the incident without the LEA's prior written approval, except as strictly required by law.

10. Data Retention, Return & Destruction

The Provider retains Student Data only as long as needed to provide the Service or as directed by the LEA. Student photos captured for ticket verification are automatically purged no later than three (3) days after the associated event ends or seven (7) days after upload, whichever occurs first. Upon expiration or termination of the Agreement, or at the LEA's written request, the Provider will return and/or securely destroy Student Data within thirty (30) days (or such longer period as the parties may agree in writing if volume or complexity reasonably requires) and, on request, certify destruction — except De-Identified Data and data the Provider is required by law to retain.

11. Compelled Disclosure

If the Provider is legally compelled to disclose Student Data, it will, unless prohibited by law, give the LEA prompt notice so the LEA may seek a protective order, and disclose only the minimum required.

12. De-Identified Data

The Provider may use De-Identified Data to operate, maintain, and improve the Service and for aggregate reporting, provided it does not attempt to re-identify students and does not release De-Identified Data in a manner that could reasonably identify a student.

13. Term; Survival; Governing Law; Miscellaneous

This Addendum is effective on the last signature date and continues while the Provider holds Student Data. Sections 4–12 survive termination.

- **Governing Law and Venue:** This Addendum shall be governed by and construed in accordance with the laws of the State of Texas, without regard to its conflict of laws principles, except that with respect to Student Data privacy and security claims arising under state student data privacy laws, the laws of the state in which the LEA is located shall apply to the extent they provide greater protection to the LEA or students. Venue for

any disputes shall lie in the state or federal courts located in Potter County, Texas, or, at the LEA's election for privacy-related claims, the courts of the LEA's jurisdiction.

- **State-Specific Requirements:** To the extent the LEA is subject to additional state student data privacy laws (including but not limited to New York Education Law § 2-d, which requires a Data Security and Privacy Plan and compliance with the Parents' Bill of Rights for Data Privacy and Security; California's Student Online Personal Information Protection Act (SOPIPA) and related provisions such as AB 1584; or analogous laws in other states), the parties agree to execute any required state-specific addendum, rider, or supplemental terms, or to incorporate such terms by reference. Provider will comply with all applicable additional requirements and will provide reasonable assistance to the LEA in fulfilling its obligations under such laws.
- **Indemnification:** Provider shall indemnify, defend, and hold harmless the LEA and its officers, employees, and agents from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or related to Provider's or its Subprocessors' breach of this Addendum or unauthorized access, use, or disclosure of Student Data, to the extent caused by Provider's negligence, willful misconduct, or material breach. Any limitation of liability or exclusion of consequential damages in the Agreement shall not apply to claims arising from breach of this Addendum, gross negligence, or willful misconduct with respect to Student Data, or to the extent prohibited by applicable law; provided, however, that except in cases of gross negligence or willful misconduct, Provider's aggregate liability for all claims arising under this Addendum shall not exceed the greatest of (i) the total fees paid by LEA to Provider in the twelve (12) months preceding the claim, (ii) the per-occurrence limit of Provider's applicable cyber liability insurance policy then in effect, or (iii) one hundred thousand dollars ($100,000).
- **Insurance:** Upon the LEA’s request, or as required by applicable state law, Provider shall obtain and maintain commercial general liability insurance and cyber liability / data breach insurance with coverage limits reasonably acceptable to the LEA, including coverage for privacy liability, network security, and notification costs. Provider shall provide certificates of insurance to the LEA upon request.

Signatures

Its One App, LLC By: _____Name/Title: _____ Date: _____

LEA: _____ By: _____
Name/Title: _____ Date: _____

Exhibit A — Categories of Student Data Processed

Depending on how the LEA configures its events, the Service may process:

- Student/attendee name; guardian/purchaser name, email, phone
- Date of birth; grade level [if collected by the LEA via custom fields]
- Emergency contact and health/medical notes [if collected via custom fields; flag these fields as "sensitive" in the event builder]
- Sport/team details (position, jersey number, sizes) [if collected]
- Ticket verification photo [if the LEA enables photo tickets]
- Ticketing/transaction metadata (order, event, timestamps)

IMPORTANT NOTE: The content of custom registration fields is controlled by the LEA. The LEA should collect only the minimum Student Data needed and mark medical/DOB/ID fields as Sensitive in the event builder. The LEA is solely responsible for ensuring that its collection and use of any Student Data (including via custom fields) complies with FERPA, applicable state laws, and any required parental notices or consents. Provider tools (including sensitive-field marking) are provided to assist the LEA in meeting these obligations.

Exhibit B — Subprocessors

Provider confirms that appropriate Data Processing Agreements or equivalent contractual terms are in place with each Subprocessor listed below, flowing down obligations substantially equivalent to those in this Addendum with respect to Student Data processed by such Subprocessor, including limitations on use, security safeguards, breach notification, and deletion/return rights. Provider will update this Exhibit B as Subprocessors change and provide the updated version to LEA.

Subprocessor	Function	Data
Supabase	Cloud database, authentication, file storage	All platform data
Cloudflare R2	Access-controlled storage for ticket photos	Student photos
Stripe	Payment processing and payouts	Purchaser/payment data (transactional only; no education records used for marketing or profiling)
Resend	Transactional email (receipts, tickets)	Purchaser email + ticket info
Apple (PassKit)	Apple Wallet pass generation	Ticket/pass metadata
Vercel	Application hosting, serverless compute, and cron scheduling	All HTTP requests and server-side rendering pass through Vercel infrastructure
Google (Gemini AI)	AI-powered administrative support chatbot (admin-only; not accessible to students or parents)	Admin questions and org metadata only; no Student Data is sent to the Gemini API
Google	Optional Google sign-in; Google Wallet pass generation	Auth identifiers; Wallet pass metadata

Provider contact for privacy/DPA requests: privacy@its1app.com
Date: July 14, 2026
Steven Singleton / Michael Keough
Co-Founders & Member-Managers
Its One App, LLC