Data Privacy Agreement

Last updated: May 6, 2026

This Data Privacy Agreement ("DPA") is based on the National Data Privacy Agreement (NDPA), Version 2.2, authored by members of the Student Data Privacy Consortium (SDPC) and Mark Williams, Fagen, Friedman & Fulfrost LLP. It governs the handling of Student Data between participating educational institutions ("LEA") and Downbeat LLC ("Provider").

> **For schools and districts:** To enter into this DPA with Downbeat LLC, complete the LEA fields in the signature block and return a countersigned copy to mason@downbeatapp.com. Downbeat's General Offer of Privacy Terms (Exhibit E) means any LEA may execute this DPA under these same terms without individual negotiation.

Parties

LEA (School / District)	[Full legal name of institution — completed at signing]
LEA Address	[Street, City, State, Zip — completed at signing]
LEA Representative	[Name, title, email — completed at signing]
Provider	Downbeat LLC
Provider Address	34 March Ave, Brookville, OH 45309
Provider Representative	Mason Combs, Founder & CEO — mason@downbeatapp.com
Security Contact	Mason Combs — mason@downbeatapp.com

Special Provisions: [ ] If checked, the Supplemental State Terms attached hereto as Exhibit G are hereby incorporated by reference into this DPA in their entirety.

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the date of last signature below.

LEA: [School / District Name]	**Provider: Downbeat LLC**
Signature:	Signature:
_____	_____
Printed Name:	Printed Name: Mason Combs
_____	_____
Title / Position:	Title / Position: Founder & CEO
_____	_____
Date:	Date:
_____	_____

Preamble

WHEREAS, the Provider is providing educational or digital Services, as defined in Exhibit A, to the LEA, which Services include (a) cloud-based Services for the digital storage, management, and retrieval of Student Data; and/or (b) digital educational software that authorizes Provider to access, store, and use Student Data; and

WHEREAS, the Provider and LEA have entered into a Service Agreement to provide certain Services to the LEA as set forth in the Service Agreement and this DPA (collectively, the "Agreement");

WHEREAS, the Provider and LEA recognize the need to protect Student Data 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 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h; and the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501–6506 (16 C.F.R. Part 312);

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.

Standard Clauses

Article I: Purpose and Scope

1.1 Purpose of DPA. The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal and state privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, performing Services otherwise provided by the LEA. With respect to its use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA as set forth in this DPA and the Service Agreement.

1.2 Description of Products and Services. A description of all products and services covered by the Agreement is listed in Exhibit A. Provider may add or delete products or services subject to this DPA under the following circumstances:

- Deleted products or services: The products or services have been discontinued and are no longer available from the Provider.
- Added products or services: The added products or services are a direct replacement for, or substantially equivalent to, the original products or services listed in the DPA; or the added products or services result in new or enhanced capabilities, new modules, or technology advancements relating to the listed products or services.

Provider must notify the LEA of any Addendum modifying Exhibit A. The LEA will have thirty (30) days from receipt to object in writing to the Addendum. If no written objection is received it will become incorporated into the DPA.

1.3 Student Data to Be Provided. In order to perform the Services, the Provider shall process Student Data as identified in the Schedule of Data, attached hereto as Exhibit B. If a Provider needs to update any information on Exhibit B, they may do so by completing an Addendum and sending a copy to the LEA. The LEA will have thirty (30) days from receipt to object. If no written objection is received it will become incorporated into the DPA.

1.4 DPA Definitions. Capitalized terms used in this DPA shall have the meanings set forth in Exhibit C.

Article II: Data Ownership and Authorized Access

2.1 Student Data Property of LEA. As between LEA and Provider, all Student Data processed by the Provider pursuant to the 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 processed by the Provider, including any modifications or additions or any portion thereof

from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. All rights, including all intellectual property rights in and to Student Data, shall remain the exclusive property of the LEA.

2.2 Parent, Legal Guardian, and Student Access. The LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data and request deletion or modification. Provider shall establish reasonable procedures by which the LEA may access and correct Education Records and Student Data. Provider shall respond to LEA requests within thirty (30) days. In the event that any person other than authorized users contacts the Provider about Student Data, the Provider shall refer that person to the LEA.

Where the LEA has chosen to designate specific parents or legal guardians as authorized to view a particular student's records through Provider's Guardian Portal, such access constitutes a permitted disclosure by the LEA on its own behalf, made through Provider as School Official. The LEA retains responsibility for designating which guardians are authorized for which students and for revoking access when no longer appropriate. Provider shall provide the LEA with administrative tools to grant, revoke, and audit Guardian Portal access at any time.

2.3 Subprocessors. Provider shall enter into a Subprocessor Agreement with all Subprocessors performing functions for the Provider, whereby Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA. Every Subprocessor Agreement must provide that the Subprocessor will not sell the Student Data.

Article III: Duties of LEA

3.1 Provide Data in Compliance with Applicable Laws. LEA shall use the Services and provide Student Data in compliance with all applicable federal and state privacy laws, rules, and regulations.

3.2 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.

3.3 Reasonable Precautions. LEA shall employ administrative, physical, and technical safeguards designed to protect usernames, passwords, and any other means of gaining access to the Services and/or hosted Student Data from unauthorized access, disclosure, or acquisition.

3.4 Unauthorized Access Notification. LEA shall notify Provider within seventy-two (72) hours of any confirmed Data Breach to the Services, LEA's account, or any Student Data that poses a privacy or security risk. LEA will provide reasonable assistance to Provider in any efforts to investigate and respond to such Data Breach if requested.

Article IV: Duties of Provider

4.1 Privacy and Security Compliance. The Provider shall comply with all laws and regulations applicable to Provider's protection of Student Data privacy and security, and at the direction of the LEA shall cooperate with any state or federal government-initiated audit of the LEA's use of the Services.

4.2 Authorized Use. Student Data processed pursuant to the Services shall be used by the Provider for no purpose other than performing the Services outlined in Exhibit A, or as instructed by the LEA.

4.3 Provider Employee Obligation. Provider shall require all employees who have access to Student Data to comply with all applicable provisions of this DPA. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee with access to Student Data pursuant to the Service Agreement.

4.4 No Disclosure. Provider acknowledges and agrees that it shall not sell or disclose any Student Data or any portion thereof, including Personally Identifiable Information contained in the Student Data. Exceptions to this prohibition include:

- Disclosure directed or permitted by the LEA or this DPA;
- Disclosure pursuant to a judicial order or lawfully issued subpoena or warrant (Provider shall notify LEA in advance where legally permissible);
- Disclosure to Subprocessors performing Services on behalf of the Provider pursuant to this DPA;
- Disclosure to LEA-authorized users of the Services, which may include parents and legal guardians authenticated through Provider's Guardian Portal where the LEA has designated them as authorized to view the relevant Student Data;
- Disclosure to protect the safety of users or others, where required by applicable law.

4.5 De-Identified Data. Provider agrees not to attempt to re-identify De-Identified Data without the written direction of the LEA. De-Identified Student Data may be used by the Provider for research and development purposes and to demonstrate the effectiveness of the Services. Provider agrees not to transfer De-Identified Data to any third party unless the transfer is expressly directed or permitted by the LEA or this DPA.

4.6 Disposition of Student 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. At the termination of this DPA, the Provider shall dispose of or delete Student Data obtained by the Provider under the Agreement within sixty (60) days of termination unless otherwise required by law. Provider will provide written confirmation of deletion upon LEA request.

4.7 Advertising Limits. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; (b) develop a profile of a student, family member/guardian, or group, for any purpose other than providing the Service to LEA; or (c) for any commercial purpose other than to provide the Service to the LEA. Targeted Advertising is strictly prohibited.

Article V: Data Security and Breach Provisions

5.1 Data Storage. Student Data is stored exclusively within the United States. See Exhibit B for storage location details.

5.2 Security Audits. Provider will conduct a security audit or assessment no less than once per year, and upon a Data Breach. Upon 10 days' notice and execution of a confidentiality agreement, Provider will provide the LEA with a summary of the audit report, subject to reasonable and appropriate redaction.

5.3 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 implement an adequate Cybersecurity Framework that incorporates one or more of the nationally or internationally recognized standards set forth in Exhibit F. Provider's security contact information is provided in the Parties section of this DPA.

5.4 Data Breach. In the event that Provider confirms a Data Breach, the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the Data Breach, unless notification within these time limits would disrupt investigation of the Data Breach by law enforcement. The Data Breach notification shall include, at a minimum:

- The name and contact information of the Provider;
- The date of the notice and the date or date range of the Data Breach;
- Whether notification was delayed as a result of a law enforcement investigation, if legally permissible to share;
- A general description of the Data Breach;
- A description of the Student Data reasonably believed to have been affected; and
- Identification of impacted individuals.

Provider agrees to adhere to all applicable federal and state laws with respect to a Data Breach related to Student Data. Provider shall maintain a written Data Breach response plan consistent with applicable industry standards and agrees to provide LEA, upon reasonable written request, with a summary of said plan.

Contract Terms

Term and Termination. In the event that either Party seeks to terminate this DPA, they may do so by written notice if the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any Service Agreement if the other party breaches any terms of this DPA. This DPA shall stay in effect for as long as the Provider retains the Student Data.

Data Disposition on Service Agreement Termination. If the Service Agreement is terminated, the Provider shall dispose of all of LEA's Student Data pursuant to Article IV, Section 4.6.

Priority of Agreements. This DPA shall govern the treatment of Student Data in order to comply with applicable privacy protections. In the event of a conflict between the terms of the DPA and the Service Agreement, Terms of Service, or Privacy Policies, the terms of this DPA shall apply and take precedence with respect to Student Data.

Governing Law. 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 to the sole and exclusive jurisdiction of the state and federal courts for the county of the LEA for any dispute arising out of or relating to this DPA.

Entire Agreement. This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersede all prior communications, representations, or agreements relating thereto. This DPA may be amended only with the signed written consent of both Parties.

Successors Bound. This DPA is binding upon the respective successors in interest to Provider in the event of a Change of Control. Provider shall provide written notice to LEA no later than sixty (60) days after the closing date of any Change of Control.

Authority. Each signatory confirms they are authorized to bind their institution to this DPA in its entirety.

Exhibit A: Products and Services

This DPA covers access to and use of Downbeat LLC's existing Services described below that collect, process, or transmit Student Data.

Field	Details
Product Name	Downbeat — Band Program Management Platform

Website	https://www.downbeatapp.com
Description	Cloud-based inventory and program management system for marching and concert band programs. Provides uniform and instrument tracking, student roster management, checkout/checkin workflows, damage reporting, repair tracking, equipment assignment records, fee tracking, and a Guardian Portal that allows LEA-designated parents and guardians to view records relating to their student via magic-link authentication.
Type of Service	Cloud-based SaaS application — digital storage, management, and retrieval of Student Data on behalf of LEA, including LEA-directed disclosure of Student Data to authorized parents and guardians via the Guardian Portal.
Data Storage Location	United States only — Supabase (AWS us-east-1). No Student Data is stored outside the United States.
Provider Address	34 March Ave, Brookville, OH 45309

Subprocessors

Provider engages the following subprocessors to deliver the Services. Each has entered into a data processing agreement with Provider consistent with the terms of this DPA.

Subprocessor	Purpose	Data Location
Supabase, Inc.	Database, authentication, and file storage	United States (AWS us-east-1)
Vercel, Inc.	Application hosting and delivery	United States
Resend, Inc.	Transactional email notifications, including Guardian Portal magic-link emails	United States
Stripe, Inc.	Payment processing (billing data only — no Student Data transmitted)	United States

Exhibit B: Schedule of Student Data

All data elements identified in this Exhibit are correct at time of signature. R = Required for service delivery. O = Optional, provided at LEA discretion. No = Not collected.

Data Element	Collected	R / O
Student Identity Data		
Student first name	Yes	R
Student last name	Yes	R
Student email address	Yes (if provided by LEA)	O
Band section / ensemble assignment	Yes	R
Academic year / season	Yes	R
Student ID number (if imported from LEA system)	Yes (if provided by LEA)	O
Equipment and Inventory Assignment Records		
Uniform piece identifier / asset tag	Yes	R
Uniform type (jacket, pants, shako, etc.)	Yes	R
Uniform size data (chest, waist, inseam, etc.)	Yes (if provided by LEA)	O
Instrument identifier / asset tag	Yes (if applicable)	O
Instrument type and model	Yes (if applicable)	O
Assignment date and return date	Yes	R
Condition at checkout / check-in	Yes	R
Damage report notes and photos	Yes (if submitted)	O
Fee and Payment Records		
Fee obligations (amount, due date, fee type)	Yes (if LEA uses budget module)	O
Payment status and amounts paid	Yes (if LEA uses budget module)	O
Parent / Guardian Contact Information (provided by LEA)		
Guardian first and last name	Yes (if provided by LEA)	O

Guardian email address	Yes (if provided by LEA; required for Guardian Portal access)	O
Guardian phone number	Yes (if provided by LEA)	O
Guardian-to-student relationship designation	Yes (if provided by LEA)	O
Guardian Portal Authentication Data (collected by Provider for security only)		
Magic-link tokens (hashed, 15-minute expiry)	Yes	R for Guardian Portal access
Session tokens (hashed, 30-day expiry)	Yes	R for Guardian Portal access
IP address and user-agent at time of authentication (security only; not surfaced to LEA)	Yes	R for Guardian Portal access
Data NOT Collected by Downbeat LLC		
Social Security Number	No	—
Date of birth	No	—
Home address	No	—
Grade level / GPA / academic performance	No	—
Disciplinary records	No	—
Health or medical information	No	—
Race, ethnicity, or demographic data	No	—
Biometric data	No	—

Payment card details are not collected by Provider. Where the LEA enables fee payment links, payments are processed by external platforms (Venmo, PayPal, Cash App) chosen by the LEA, which are governed by their own terms and privacy policies and which do not transmit payment card data back to Provider.

Exhibit C: Definitions

"Student Data" means any data or information about a student that is submitted to, created by, or generated through use of the Services, and that constitutes an education record under FERPA or is otherwise subject to applicable student privacy law.

"De-Identified Data" means data from which all direct and indirect personal identifiers have been removed such that it cannot reasonably be used to identify an individual student, consistent with NIST de-identification standards or U.S. Department of Education guidance.

"Data Breach" means any confirmed unauthorized acquisition, use, disclosure, modification, or loss of Student Data that compromises the security, confidentiality, or integrity of such data.

"Provider" means Downbeat LLC, located at 34 March Ave, Brookville, OH 45309.

"LEA" (Local Education Agency) means the school, school district, or educational institution that has entered into a Service Agreement with Provider and is executing this DPA.

"School Official" means Provider acting in an official capacity on behalf of the LEA with a legitimate educational interest in the Student Data, consistent with 34 C.F.R. § 99.31(a)(1).

"Service Agreement" means the terms of service, subscription agreement, or other contract between Provider and LEA governing access to and use of the Services.

"Subprocessor" means any third party engaged by Provider to process Student Data on Provider's behalf in connection with delivering the Services.

"Targeted Advertising" means presenting advertisements to a student based on information obtained or inferred from that student's use of the Services, where such advertising is not contextual to the Services.

"Change of Control" means any merger, acquisition, or transfer of all or substantially all of the assets of Provider.

"Guardian Portal" means the feature of the Services that allows adult parents, legal guardians, or other contacts designated by the LEA to authenticate via single-use magic link and view Student Data the LEA has authorized them to view for a specific student.

Exhibit D: Data Disposition Instructions

Upon termination of the Service Agreement or written request by LEA, Downbeat LLC will follow this data disposition procedure:

- Provider will make available to LEA a full export of all Student Data in CSV or Excel format within sixty (60) days of the written request or termination date.
- Provider will permanently delete all Student Data from Provider's systems — including Supabase database records, uploaded files, application logs, and Guardian Portal session and token records — within sixty (60) days of the export being confirmed as received by LEA, or within sixty (60) days of termination if LEA does not request an export.
- Provider will instruct all Subprocessors (Supabase, Vercel, Resend) to delete applicable Student Data in accordance with their respective data processing agreements.
- Provider will provide written confirmation of deletion to LEA within ten (10) business days of completion upon request.
- De-Identified aggregate data, if any exists, may be retained by Provider consistent with applicable law and Section 4.5 of the Standard Clauses.

Exhibit E: General Offer of Privacy Terms

By executing this DPA, Downbeat LLC makes a general offer of the privacy terms contained herein to all LEAs. Any LEA may enter into this DPA with Downbeat LLC by completing the Parties section and signature block and delivering a countersigned copy to Provider. This general offer remains in effect unless and until Provider provides written notice of withdrawal.

Field	Details
Provider Name	Downbeat LLC
Authorized Signatory	Mason Combs, Founder & CEO
Date of General Offer	May 6, 2026

To execute this DPA, contact mason@downbeatapp.com or download the DPA using the link at the top of this page.

Exhibit F: Cybersecurity Framework and Security Measures

Downbeat LLC implements the following administrative, physical, and technical safeguards to protect Student Data. Provider aligns its security program with the NIST Cybersecurity Framework (CSF) core functions: Identify, Protect, Detect, Respond, and Recover.

Technical Safeguards

- All Student Data encrypted at rest using AES-256 (via Supabase on AWS infrastructure)
- All data encrypted in transit using TLS 1.2 or higher
- Authentication for Account Holders managed by Supabase Auth (SOC 2 Type II certified)
- Authentication for Guardian Portal Users by single-use, time-limited magic link sent to an email address designated by the LEA. Guardians do not maintain passwords. Magic link tokens and session tokens are stored only in hashed form. Magic links expire after fifteen (15) minutes; sessions expire after thirty (30) days of inactivity. The LEA may revoke any active guardian session at any time through the administrative interface.
- Per-IP and per-guardian rate limiting on Guardian Portal magic link requests and consumption to prevent brute-force or enumeration attacks
- Row-level security (RLS) enforced at the database layer — each organization's data is logically isolated and inaccessible to other organizations
- Role-based access controls within the application limit access to authorized LEA personnel only
- Application credentials and API keys stored in encrypted environment variables, never in source code or version control
- Application deployed exclusively over HTTPS via Vercel with automatic certificate management
- All file storage (including damage report photos) managed through Supabase Storage with access controls tied to authenticated sessions
- Guardian Portal IP addresses, user-agent strings, and authentication timestamps are retained solely for security and rate-limiting purposes and are not exposed to the LEA, Account Holders, or any other party

Administrative Safeguards

- Access to production systems is limited to authorized personnel of Downbeat LLC
- Data Processing Agreement executed with Supabase, Inc.
- Subprocessor terms in place with Vercel, Resend, and Stripe consistent with this DPA

- Provider maintains a written Data Breach response plan consistent with Section 5.4 of this DPA; a summary is available to LEA upon written request
- Annual internal security review conducted against the NIST CSF checklist, with results documented and available to LEA upon written request
- The LEA controls Guardian Portal designations: the LEA selects which parents or guardians may access which students' records and may revoke access at any time. Provider does not unilaterally grant Guardian Portal access.

Physical Safeguards

- No Student Data is stored on local devices or physical media outside of cloud infrastructure
- Cloud infrastructure physical security provided by AWS (SOC 2, ISO 27001 certified data centers)

Exhibit G: Supplemental State Terms

Supplemental State Terms are incorporated only when the checkbox in the Preamble is marked and the applicable state's terms are attached as an addendum to this DPA. If no checkbox is marked, this Exhibit does not apply.