



Data Privacy Agreement

Agreement for Texas school district partnerships

PARTIES

District

District legal name

Authorized representative (name)

Title

Provider

EvalCamp (NetDev Studio, LLC)

Robert Arellano, Co-Founder

Austin, Texas

Effective Date: _____

Article I Definitions

1.1 "Student Data" means personally identifiable information (PII) from education records as defined by the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g, and its implementing regulations at 34 CFR Part 99, that is provided to or collected by the Provider on behalf of the District through the use of the Provider's services.

1.2 "Education Records" means those records that are directly related to a student and are maintained by an educational agency or institution, or by a party acting for the agency or institution, as defined by FERPA (34 CFR §99.3).

1.3 "Personally Identifiable Information (PII)" includes, but is not limited to: the student's name; the name of the student's parent or other family members; the address of the student or student's family; a personal identifier such as the student's Social Security number, student number, or biometric record; other indirect identifiers such as the student's date of birth, place of birth, and mother's maiden name; and other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community to identify the student with reasonable certainty (34 CFR §99.3).

1.4 "Authorized Representative" means an individual designated by the District to act on its behalf with respect to this Agreement.

1.5 "Breach" means the unauthorized acquisition, access, use, or disclosure of Student Data that compromises the security, confidentiality, or integrity of the Student Data.

1.6 "Service" means the EvalCamp evaluation workflow management platform and related services provided by the Provider to the District.

Article II Purpose

2.1 The purpose of this DPA is to describe the obligations and responsibilities of the Provider and the District with respect to the protection of Student Data that the Provider may receive, collect, or process in connection with providing the Service to the District.

2.2 The Provider offers a cloud-based evaluation workflow management platform that enables the District's special education staff to track evaluation timelines, coordinate tasks, and distribute forms to parents and teachers. The Service is a coordination and visibility tool and does not process IEP documents, assessment results, clinical reports, or educational testing data.

Article III Student Data to Be Provided

3.1 The District will provide, or the Provider will collect on behalf of the District, only the following categories of Student Data:

Data Category	Specific Elements	Purpose
Student identification	First name, last name, ID	Associate evaluations with the correct student
Student enrollment	Grade level, campus assignment	Organize evaluations by grade and campus
Parent/guardian contact	Name, email address, preferred language	Distribute evaluation-related forms
Teacher contact	Name, email address	Distribute evaluation-related forms
Evaluation workflow	Task titles, status, due dates, completion dates	Track evaluation workflow progress
Form tracking	Form title, form URL (link only), send date, completion status	Track form distribution and completion

3.2 The Provider will not collect Student Data beyond what is enumerated above without prior written consent from the District.

3.3 The Provider does not collect or process: Social Security numbers, student ID numbers, dates of birth, home addresses, disability categories, assessment scores, IEP documents, medical or health records, behavioral records, attendance data, disciplinary records, or document attachments of any kind. Forms are tracked by URL only — the Provider does not access, store, or process form content or responses.

Article IV Data Use Restrictions

4.1 The Provider shall use Student Data solely for the purpose of providing the Service to the District as described in this Agreement.

4.2 The Provider shall not use Student Data for any purpose other than providing the Service, including but not limited to:

- (a) Targeted advertising directed at students or parents
- (b) Building or supplementing commercial profiles of students
- (c) Selling, renting, or leasing Student Data to any third party
- (d) Data mining or data analytics for non-educational commercial purposes
- (e) Any use not authorized by the District

4.3 The Provider shall not disclose Student Data to any third party without the prior written consent of the District, except as required by law or as specified in Article IX (Subprocessors).

4.4 The Provider shall not use Student Data to engage in any activities prohibited by FERPA, Texas Education Code §32.151, Texas HB 2087, or any other applicable federal or state law.

Article V Data Security

5.1 The Provider shall implement and maintain reasonable administrative, technical, and physical safeguards to protect Student Data from unauthorized access, acquisition, destruction, use, modification, or disclosure.

5.2 The Provider's security measures include, at minimum:

- (a) Encryption in transit — All data transmitted between users and the Service is encrypted using TLS/HTTPS (SSL)
- (b) Encryption at rest — All Student Data stored in the database and on disk is encrypted
- (c) Authentication — Secure user authentication with encrypted password storage
- (d) Role-based access control — Access to Student Data is limited by user role (administrator, staff) as configured by the District
- (e) US-based hosting — All Student Data is stored and processed in data centers located in the United States (Ashburn, Virginia)
- (f) Automated backups — Daily automated database backups
- (g) Access restrictions — Production server and database access is limited to authorized Provider personnel

5.3 The Provider shall periodically review and update its security practices to address emerging threats and industry best practices.

Article VI Data Ownership

6.1 The District retains sole ownership of all Student Data. The Provider acquires no rights to Student Data other than the limited right to process the data as specified in this Agreement.

6.2 The Provider holds Student Data as a custodian and fiduciary on behalf of the District.

6.3 Nothing in this Agreement shall be construed as granting the Provider any intellectual property rights in Student Data.

Article VII Data Retention and Destruction

7.1 The Provider shall retain Student Data only for the duration of this Agreement and for a period not to exceed thirty (30) calendar days following its termination, subject to the backup-purge timeline set out in Section 7.2.

7.2 Upon termination or expiration of this Agreement, or upon written request by the District:

- (a) The Provider shall export and deliver all Student Data to the District in a standard, machine-readable format (CSV) within fifteen (15) calendar days of the request;
- (b) The Provider shall permanently delete all Student Data from its active production systems within thirty (30) calendar days of termination;
- (c) Residual copies of Student Data contained in the Provider's encrypted, rolling system backups shall be overwritten and purged in the ordinary course of the Provider's backup rotation, and in no event later than sixty (60) calendar days following termination. During this interval such backup copies remain encrypted and are not accessed except as necessary for disaster recovery;
- (d) The Provider shall provide written certification of destruction to the District within ten (10) business days after the backup-purge period described in Section 7.2(c) is complete.

7.3 The Provider shall not retain any Student Data in any form after the periods described in Section 7.2, except as required by applicable law.

Article VIII Breach Notification

8.1 The Provider shall notify the District in writing within seventy-two (72) hours of the Provider's discovery of a Breach involving Student Data.

8.2 The breach notification shall include, to the extent known at the time of notification:

- (a) The nature and scope of the Breach
- (b) The categories and approximate number of students affected
- (c) The specific Student Data elements involved
- (d) A description of the measures taken or proposed to be taken to address the Breach
- (e) Recommended actions for the District to mitigate potential harm

8.3 The Provider shall cooperate fully with the District in investigating and remediating any Breach, including providing any additional information or documentation requested by the District.

8.4 The Provider shall comply with all applicable breach notification requirements under Texas law and FERPA.

Article IX Subprocessors

9.1 The Provider uses the following third-party subprocessors in connection with the Service:

Subprocessor	Service Provided	Data Accessed
Resend	Transactional email delivery	Recipient email address and email content for form distribution and notification emails
Hetzner Cloud	Infrastructure hosting	All Student Data (encrypted at rest and in transit)
DigitalOcean	Database backup storage	All Student Data (encrypted)
Gleap	Customer support platform	User-submitted support messages, screenshots, and metadata (may include Student Data if referenced in a support request)
Jitsu & PostHog	Product analytics	Anonymized usage events, page views, and feature interactions (no direct Student Data)
AppSignal	Error reporting and application monitoring	Application error logs and performance metrics (does not include Student Data in error context)

9.2 The Provider shall not engage additional subprocessors that will have access to Student Data without providing the District with prior written notice and an opportunity to object.

9.3 The Provider shall ensure that all subprocessors are contractually bound to data protection obligations no less protective than those set forth in this Agreement.

Article X Access and Audit Rights

10.1 The District may request a full export of its Student Data at any time during the term of this Agreement. The Provider shall fulfill such requests within fifteen (15) calendar days.

10.2 The District may, upon reasonable written notice, audit the Provider's data privacy and security practices as they relate to Student Data under this Agreement.

10.3 The Provider shall respond to reasonable inquiries from the District regarding its data privacy and security practices within ten (10) business days.

Article XI FERPA Compliance

11.1 The Provider is designated as a "school official" with a "legitimate educational interest" under FERPA (34 CFR §99.31(a)(1)(i)), as the Provider performs an institutional service or function for which the District would otherwise use its own employees.

11.2 The Provider is under the direct control of the District with respect to the use and maintenance of education records, as the District determines what Student Data is entered, who has access, and how the Service is used.

11.3 The Provider shall use PII from education records only for the purposes authorized by the District under this Agreement.

11.4 The Provider shall not re-disclose PII from education records to any third party without the prior written authorization of the District, except as required by law.

11.5 The Provider shall comply with all applicable provisions of FERPA and its implementing regulations at 34 CFR Part 99.

Article XII Texas State Law Compliance

12.1 The Provider shall comply with all applicable Texas laws and regulations pertaining to student data privacy and confidentiality, including but not limited to:

- (a) Texas Education Code §32.151 et seq. (Texas Student Privacy Act / SB 1792)
- (b) Texas HB 2087 (Education Service Provider requirements)
- (c) Texas Government Code Chapter 560 (as applicable)

12.2 In accordance with Texas Education Code §32.151, the Provider shall not:

- (a) Use Student Data for targeted advertising
- (b) Use a student's academic performance to market commercial products
- (c) Sell Student Data to any third party
- (d) Create commercial profiles of students based on Student Data

12.3 The Provider shall maintain compliance with any future amendments to Texas student data privacy laws that become effective during the term of this Agreement.

Article XIII Indemnification

13.1 The Provider shall indemnify, defend, and hold harmless the District from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising from or related to:

- (a) The Provider's breach of this Agreement
- (b) The Provider's negligent or unauthorized use or disclosure of Student Data
- (c) Any Breach of Student Data caused by the Provider's failure to maintain reasonable security measures

13.2 This indemnification obligation shall survive the termination of this Agreement.

13.3 Limitation. Except in cases of the Provider's gross negligence, willful misconduct, or fraud, the Provider's total aggregate liability under this Article XIII shall not exceed the greater of (a) the total fees paid or payable by the District to the Provider under the applicable service agreement during the twelve (12) months preceding the event giving rise to the claim, or (b) the limits of the Provider's cyber-liability and technology errors-and-omissions insurance applicable to the claim.

Article XIV Term and Termination

14.1 This DPA shall be co-terminus with the service agreement between the District and the Provider for the EvalCamp Service.

14.2 Either Party may terminate this Agreement with thirty (30) days' written notice to the other Party.

14.3 The data destruction obligations in Article VII shall survive termination of this Agreement.

14.4 The breach notification obligations in Article VIII, the indemnification obligations in Article XIII, and the confidentiality obligations throughout this Agreement shall survive termination.

Article XV General Provisions

15.1 Amendments — This Agreement may only be amended by written agreement signed by both Parties.

15.2 Governing Law — This Agreement shall be governed by and construed in accordance with the laws of the State of Texas.

15.3 Severability — If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect.

15.4 Entire Agreement — This DPA, together with any service agreement between the Parties, constitutes the entire agreement between the Parties with respect to the subject matter hereof.

15.5 Notices — All notices required under this Agreement shall be in writing and sent to the addresses listed on the cover page, or to such other address as a Party may designate in writing.

SIGNATURES

By signing below, each Party acknowledges that it has read, understood, and agrees to be bound by the terms of this Data Privacy Agreement.

District	Provider EvalCamp
 Signature	 Signature
	Robert Arellano
 Printed Name	Co-Founder
	 Date
 Title	
 Date	

Districts may substitute their own Data Privacy Agreement, including SDPC / TXSPA standard agreements. EvalCamp is committed to executing whichever agreement format the district prefers.