



STUDENT DATA PRIVACY AGREEMENT

Student Data Privacy Agreement

Between RidePermit, Inc ("Provider") and the school district named below ("District"). Template version 1.0, September 2026. Reviewed by District counsel before signature.

Draft for counsel. This agreement follows the structure of the Student Data Privacy Consortium National Data Privacy Agreement and the requirements of California Education Code section 49073.1, FERPA, COPPA, and SOPIPA. It is a template prepared by RidePermit for review by the District's legal counsel and by RidePermit's counsel before execution. It is not legal advice.

Field	Entry
District (LEA)	_____
District address	_____
District contact for this agreement	_____
Provider	RidePermit, Inc, a Delaware corporation, Rancho Santa Margarita, California
Provider contact	support@ridepermit.com, (949) 670-3802
Service	The RidePermit platform: device registration, safety training, permit issuance, decal verification, and district reporting, as described in the Service Agreement
Effective date	_____

1. Purpose and scope

The District has entered into a Service Agreement with the Provider under which the Provider operates the RidePermit platform for the District. In providing the Service, the Provider receives and processes Student Data. This Agreement governs the Provider's collection, use, protection, and disposition of that data. Where this Agreement and the Service Agreement conflict, this Agreement controls as to Student Data.

2. Definitions

- **Student Data:** Personally identifiable information from education records, and any information about a student collected through the Service, including name, date of birth, school, grade, student identifier, device details tied to a student, permit status, training records, attestations, warnings, and incident records. Student Data includes information provided by a parent or guardian about a student.
- **Parent:** The parent or legal guardian who registers a student and holds the family account.
- **De-identified Data:** Data created by the Provider from Student Data that cannot reasonably identify a student, such as counts by school or class.
- **Subprocessor:** A third party engaged by the Provider to process Student Data on the Provider's behalf, listed in Exhibit B.

3. Ownership and control of Student Data

1. Student Data is and remains the property of, and under the control of, the District. The Provider acquires no rights in Student Data beyond the limited license to process it to provide the Service.
2. The Provider processes Student Data only as directed by the District through the Service and this Agreement, and only for the purpose of providing the Service.

3. Parents may review and correct the Student Data they entered through their family account at any time. Requests to review or correct other Student Data go to the District, which directs the Provider. The Provider responds to a District direction within ten business days.
4. Content a student creates in the Service, such as training assessment responses, is Student Data. A parent may obtain a copy through the family account or by request to the District.

4. Permitted use and prohibited use

5. The Provider uses Student Data solely to provide, maintain, support, and improve the Service for the District. Improvement means product development and security; it never means marketing.
6. The Provider does not sell Student Data, rent it, or trade it.
7. The Provider does not use Student Data, or information derived from it, for targeted advertising, to build a profile of a student for any purpose other than the Service, or for any commercial purpose beyond the Service.
8. The Provider does not disclose Student Data to any third party except Subprocessors bound by terms at least as protective as this Agreement, or as required by law after notice to the District where notice is permitted.
9. The Provider does not collect a photograph of any student. Photographs of devices are not Student Data about the student's appearance and are used only for identification and recovery of the device.
10. Optional third-party registration: where a Parent expressly opts in during registration, the Provider registers the Parent's device with the Bike Index nonprofit registry in the Parent's name, transmitting device details and the Parent's email and phone only. No Student Data is transmitted. The Parent may withdraw at any time.

5. Data minimization and what is collected

The Provider collects only the data required to issue and verify a permit. Exhibit A lists every category collected. The Provider does not collect Social Security numbers, home addresses, GPS or location history, academic records, attendance, discipline records outside the Service, health records, or student photographs.

6. Public verification

The Service allows anyone to scan a permit decal and view permit status. The public verification page displays only: permit validity, school, district, device class, and expiration date. It never displays a student's name, a photograph, a parent's name, or any contact detail. Where a Parent has opted in, the page offers a contact request that connects a call through the Provider's system without disclosing the Parent's number.

7. Security

11. The Provider maintains administrative, technical, and physical safeguards appropriate to the sensitivity of Student Data, including: encryption of data in transit and at rest; row-level access controls scoping every user to their own district or school; role-based permissions; multi-factor authentication for platform administrators; audit logging of administrative and sensitive actions; and least-privilege access for Provider staff.
12. The Provider hosts the Service on infrastructure certified to SOC 2 Type II. Vendor reports are available to the District on request under confidentiality.
13. The Provider trains its personnel on student data privacy and limits access to Student Data to personnel who need it to provide support.
14. The Provider maintains a written security practices document, provided to the District, and updates the District when material changes are made.

8. Breach notification

15. If the Provider becomes aware of an unauthorized disclosure of, or access to, Student Data, the Provider notifies the District in writing without unreasonable delay and in any case within seventy-two hours of confirming the incident, with the nature of the incident, the data involved, the students affected, and the steps taken.

16. The District determines whether and how affected parents and students are notified, consistent with applicable law. The Provider cooperates fully, including by providing notice on the District's behalf at the District's direction and at the Provider's expense where the incident arose from the Provider's breach of this Agreement.
17. The Provider preserves relevant records and provides the District a post-incident report within thirty days.

9. Retention, return, and deletion

18. The District may export all Student Data at any time, at no cost, in a standard machine-readable format, through the Service.
19. On termination or expiration of the Service Agreement, the Provider makes a complete export available to the District and, within sixty days after termination unless the District directs otherwise in writing, deletes all Student Data from its systems and directs Subprocessors to do the same. The Provider certifies deletion in writing on request.
20. The Provider does not retain Student Data after deletion except in encrypted backups that expire on a rolling schedule not exceeding ninety days, which are not accessed except for disaster recovery.
21. De-identified Data may be retained. It never includes fewer than ten students in any reported group.

10. Compliance with law

The Provider acts as a "school official" with a legitimate educational interest under FERPA (34 CFR 99.31(a)(1)) for the purpose of providing the Service, is under the direct control of the District with respect to Student Data, and complies with FERPA, COPPA (the District consents on behalf of parents for students under thirteen where permitted), and applicable state student privacy laws, including California Education Code sections 49073.1 and 49073.6 and the Student Online Personal Information Protection Act (SOPIPA) where the District is in California, and the equivalent statutes of the District's state.

11. Subprocessors

The Provider uses the Subprocessors listed in Exhibit B. The Provider gives the District thirty days' written notice before adding a Subprocessor that will process Student Data, and the District may object in writing. Each Subprocessor is bound by written terms at least as protective as this Agreement.

12. Audit

On reasonable notice and no more than once per year, or after a security incident, the District may review the Provider's security practices, request the Provider's current vendor certifications, and ask written questions, which the Provider answers within twenty business days.

13. Term

This Agreement is effective on the date signed and continues for as long as the Provider holds any Student Data of the District. Sections 3, 4, 8, and 9 survive termination.

14. Signatures

District	Provider
Name: _____	Name: Tony Bright
Title: _____	Title: Chief Executive Officer, RidePermit, Inc
Signature: _____	Signature: _____
Date: _____	Date: _____

Exhibit A: Data collected

Category	Elements	Source
Parent account	Name, email, phone, opt-in choices	Parent
Student	First and last name, date of birth, school, grade, student identifier if the District requires it	Parent
Device	Make, model, class, serial number, color, device photo	Parent
Permit	Permit number, status, issue and expiration dates, decal status	System
Training	Course completion, module scores, certificate identifier, or an uploaded outside certificate	System / Parent
Attestation	Parent and student acknowledgment of District rules, timestamp	Parent, student
Compliance	Warnings recorded by District staff, suspension status, stolen reports	District staff, Parent
Not collected	Student photograph, Social Security number, home address, location history, academic, attendance, health, or discipline records outside the Service	

Exhibit B: Subprocessors

Subprocessor	Purpose	Student Data processed
Supabase	Database and file storage hosting (SOC 2 Type II)	All Student Data, encrypted
Lovable	Application hosting (SOC 2 Type II)	Application runtime; Student Data in transit
Resend	Transactional email	Parent email address, permit and training notices
Twilio	Phone verification and the parent contact relay	Parent phone number; no Student Data
Stripe	Payment processing, parent-paid districts only	Parent payment details; no Student Data
Bike Index	Optional device registry, Parent opt-in only	Device details and Parent email; no Student Data
Google Analytics, Plausible	Marketing site analytics only	None; not used in the Service