Lift Off Privacy Policy

Effective Date: March 31, 2026
Operated by: Andrew Atkins and Morgan Atkins
Address: 3814 Arnold Ave, Apt 1, San Diego, CA 92104
Contact: support@lift-off.me

1. Our Commitment to Privacy

Lift Off ("we," "our," or "us"), operated by Andrew Atkins and Morgan Atkins, is committed to protecting the privacy of students, teachers, and schools that use Lift Off. Lift Off acts as a service provider or processor to schools with respect to student data, including as a "service provider" as defined under applicable state privacy laws, including the California Consumer Privacy Act (CCPA/CPRA). For purposes of this policy, "personal data" or "personal information" means information that identifies or can reasonably be linked to an individual. Our core commitments are:

- We do not sell, rent, or trade personal data. We do not sell or share personal information as those terms are defined under applicable privacy laws.
- We do not use student data for advertising or marketing.
- We do not use student data to train AI models.
- We limit data collection to what is necessary for the specific educational purpose.
- Students do not create accounts.
- No student personal data is transmitted to AI service providers.
- All AI processing occurs server-side; student devices never communicate directly with AI providers.
- We do not use third-party advertising, behavioral tracking, or profiling services.
- Schools and authorized users may request access to or deletion of data at any time.

2. Description of the Service

Lift Off is an educational tool that enables teachers to provide reading materials at appropriate levels for individual students. Teachers upload instructional content, which is adjusted for reading level and/or translated. Students access materials using a class code without creating accounts.

3. Information We Collect

Teacher Data

We collect the following information from teachers:

- Name and email address (account creation and management)
- Password (stored as hashed and salted)

- Third-party authentication data (e.g., Google or Microsoft name, email, and OAuth tokens, if SSO is used; tokens are stored securely in our database)
- Payment information (processed by Stripe; we do not store credit card numbers)
- IP address and activity logs (used for security purposes; retained for 90 days and automatically deleted thereafter)

Student Data

Students do not create accounts or enter data directly. Teachers provide:

- First name
- Reading level
- Preferred language
- Text-to-speech preference
- Student session cookie (contains only an internal student identifier and class identifier; expires after 4 hours; httpOnly, secure, SameSite=Lax)
- Class code cookie (stores only the class code string to allow frictionless re-entry; expires after 14 days; httpOnly, secure, SameSite=Lax)

We do not collect student email addresses, phone numbers, physical addresses, photos, dates of birth, or demographic data.

Note: Student cookies contain only internal identifiers (not names or other personal information), are not used as persistent identifiers, and are not used for tracking across sessions or devices. The student session cookie expires after 4 hours and is not linked to any user profile or tracking mechanism.

Classification of Student Data as Education Records

Student reading levels, preferred languages, and other data provided by teachers are treated as education records under FERPA when maintained on behalf of the school. All protections described in this policy apply to these data elements accordingly.

Educational Content

- Uploaded assignment files (e.g., PDFs, images)
- AI-generated versions of instructional content

4. How We Use Information

We use collected data solely to:

- Deliver differentiated educational content
- Enable teachers to manage classes and assignments
- Process payments
- Send essential account-related communications
- Maintain system security

We do not use personal data for advertising, profiling, or marketing.

5. AI Processing

When content is uploaded:

- Text may be extracted using optical character recognition (OCR) via Google Cloud Vision, which processes images in memory and does not persist submitted data to disk for synchronous operations.
- Text is processed via API-based AI services to adjust reading level and/or translate.
- Processed content is stored for reuse.

Important:

- Only instructional content (assignment text) is sent to AI services. Student names, reading levels, language preferences, and all other student-identifiable information are never transmitted to AI service providers.
- All AI API calls are made server-side from our infrastructure. Student devices never communicate directly with AI service providers. AI providers receive only our server's IP address, never a student's IP address.
- AI providers are prohibited by their published terms and applicable agreements from using submitted data to train or improve their models.
- Submitted instructional content may be retained by AI providers for a limited period for abuse monitoring in accordance with the provider's current API data usage policy.
- Google Cloud Vision is governed by the Google Cloud Data Processing Addendum (CDPA), which restricts Google from using customer data for any purpose other than providing the service. Google's published data usage policy confirms that submitted content is not used to train or improve Cloud Vision models.
- We maintain Data Processing Agreements (DPAs) or rely on provider Data Processing Addenda with our AI subprocessors. Where required by a customer agreement, we will execute additional DPAs with subprocessors.

6. Third-Party Service Providers (Subprocessors)

We use the following subprocessors to operate the service. All subprocessors are bound by their published terms of service, data processing addenda, and/or Data Processing Agreements (DPAs), and are restricted from using data for any purpose other than providing the services described below.

Service	Purpose	Data Shared	Notes
OpenAI	Text processing (reading level adjustment and translation)	Instructional content only — no student personal data	Prohibited by published API terms from using data for model training. Data may be retained for a limited period for abuse monitoring per provider's data usage policy.
Google Cloud Vision	OCR processing	Uploaded document images containing instructional content	Images processed in memory; not persisted to disk for synchronous

			operations. Governed by Google Cloud DPA. Published terms confirm no training on submitted data.
Stripe	Payment processing	Internal user ID and Stripe customer ID from our systems. Stripe independently collects payment details, IP address, and browser information via its hosted checkout page.	Credit card numbers not stored by us. Stripe's own collection is governed by Stripe's privacy policy.
Resend	Email delivery	Teacher name and email address	
Supabase	Primary database and file storage	Application data necessary to operate the service, including teacher account data (name, email, hashed credentials, OAuth tokens), student records (first names, reading levels, language preferences), class structures, assignments, AI-generated content, uploaded files, and activity logs	Hosted on AWS (us-east-1). Automated daily backups retained for up to 7 days.
Vercel	Application hosting	All HTTP traffic is processed through Vercel's infrastructure, including standard HTTP request metadata (such as IP addresses)	We do not intentionally log student-identifying data beyond standard HTTP request metadata, which is processed for security and operational purposes only.
Inngest	Background job processing	Assignment identifiers, internal non-direct student identifiers (not names or direct personal identifiers), reading levels, and language preferences	Can be disabled. When disabled, background processing occurs within the primary application.
Google / Microsoft	Optional SSO authentication	Teacher name and email address (only if SSO is used). OAuth tokens stored in our database.	Scopes requested: openid, email, profile (Google); openid, email, profile, User.Read (Microsoft).

We will notify users at least 30 days in advance of any material changes to our subprocessor list before those changes take effect.

7. Data Retention and Deletion

- Teacher data is retained until account deletion.
- Student data is deleted immediately upon removal by the teacher. When a student or class is deleted, all associated records (including assignment-student mappings) are permanently removed in the same transaction.
- Assignments, AI-generated content, and uploaded files are deleted immediately upon deletion by the teacher. All associated student mappings, cached content, and stored files are permanently removed at the time of deletion.
- Security logs (including IP addresses) are retained for 90 days and automatically deleted thereafter.
- Deleted data may persist in automated infrastructure backups (managed by Supabase) for up to 7 days following deletion.

Upon account deletion, all associated data — including teacher account information, student records, OAuth tokens, assignments, and generated content — is permanently removed in accordance with the timelines above. Schools and authorized users may request deletion of student data at any time, independent of account status.

8. Children's Privacy (COPPA)

Lift Off is designed for use by schools and teachers. We comply with the Children's Online Privacy Protection Act (COPPA).

- Students do not create accounts or provide data directly to Lift Off.
- Student data is provided by teachers acting on behalf of their school or district.
- Schools and districts provide consent for the collection and use of student data on behalf of students under 13, for legitimate educational purposes only, in accordance with COPPA's school-authorization exception (16 C.F.R. § 312.5(b)(1)).
- By using Lift Off, teachers represent that they are authorized by their school or district to provide student data to the service, and that such use is consistent with the school's COPPA obligations. Teachers are encouraged to confirm this authorization with their school administration before using the service.
- We do not use student data for any commercial purpose, including advertising or marketing.

If we learn that personal data has been provided directly by a child without school authorization, we will delete it promptly. To report such a concern, contact support@lift-off.me.

9. FERPA Compliance

We operate as a "school official" under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g. This designation is established through the school's or district's agreement with Lift Off (e.g., a Data Processing Agreement or Terms of Service accepted by the school), consistent with the school's annual FERPA notification to parents.

- We process student education records only for legitimate educational purposes on behalf of the school.
- Schools retain ownership and control of all student education records.

- We do not disclose student education records except as necessary to operate the service or as required by law.
- We do not share student personal data with AI providers (see Section 5).
- We do not use student education records for any purpose other than providing the contracted service.

Schools and authorized parties may request access, correction, or deletion of student education records at any time by contacting support@lift-off.me.

10. State-Specific Compliance

California (SOPIPA / AB 1584)

For California schools and districts, we comply with the Student Online Personal Information Protection Act (SOPIPA) and California Education Code § 49073.1 (AB 1584):

- We do not use student data to engage in targeted advertising.
- We do not use student data to create a profile of a student for non-educational purposes.
- We do not sell or rent student data.
- We do not disclose student data except as required to provide the service, as required by law, or as directed by the school.
- Schools retain ownership of all student data. Upon request or termination of service, we will return or delete student data in accordance with the school's instructions.
- We will notify schools of any unauthorized access to student data as required by applicable law.
- California districts may request a Data Processing Agreement (DPA) consistent with AB 1584 requirements by contacting support@lift-off.me.

New York (Education Law § 2-d)

For New York schools and districts, we comply with New York Education Law § 2-d and its implementing regulations:

- We act as an operator of a website, online service, or mobile application for educational purposes on behalf of the school.
- We do not sell or use student data for any purpose other than providing the contracted educational service.
- We implement reasonable administrative, technical, and physical safeguards appropriate to the sensitivity of the data.
- We will notify schools of any breach or unauthorized release of student data in the most expedient time possible and without unreasonable delay.
- New York schools are entitled to a Parents' Bill of Rights for Data Privacy and Security, consistent with § 2-d requirements. Schools may request this addendum by contacting support@lift-off.me.
- New York districts may request a Data Processing Agreement consistent with § 2-d requirements by contacting support@lift-off.me.

Illinois (SOPPA), Colorado, Connecticut, Virginia, and Other States

We are committed to complying with applicable state student privacy laws. If your state has enacted specific student data privacy legislation — including the Illinois Student Online Personal Protection Act (SOPPA), Colorado's Student Data Transparency and Security Act (SB 16-163), Connecticut's PA 16-189, or Virginia's student data governance provisions — please contact us at support@lift-off.me. We are committed to working with schools and districts to meet applicable state-law requirements, including by entering into state-specific data processing addenda where required.

11. International Users (GDPR)

For users in the European Economic Area, United Kingdom, or other applicable jurisdictions, the following applies:

- Legal basis for processing teacher account data: contractual necessity (to perform the service agreement).
- Legal basis for processing educational content: contractual necessity and the legitimate interests of the school in delivering differentiated instruction.
- Processing location: United States. International data transfers are subject to appropriate safeguards, including Standard Contractual Clauses where applicable.
- Data subject rights: access, rectification, erasure, restriction of processing, objection, and data portability. Requests may be submitted to support@lift-off.me and will be fulfilled within 30 days.

Note: Lift Off is intended for use by schools. If a school located in the EEA uses Lift Off, the school acts as the data controller for student data, and Lift Off acts as a data processor. We process student data only under the direction of schools acting as data controllers, and we do not knowingly process personal data of EU-resident students outside of a school-controlled data processing relationship.

If your school requires a Data Processing Agreement under Article 28 of the GDPR, please contact support@lift-off.me.

12. Data Security

We implement appropriate technical and organizational safeguards, including:

- Encryption of data in transit (TLS) and at rest at the infrastructure level (managed by Supabase)
- Hashed and salted password storage
- Access controls and authentication safeguards
- Access to personal data limited to authorized personnel with a legitimate need to access such data for service operation
- Secure file storage
- Regular security reviews and vulnerability assessments

In the event of a data breach or unauthorized access to personal data, we will notify affected schools and users as required by applicable law. For jurisdictions requiring specific notification timelines (such as GDPR's 72-hour requirement or state-specific breach notification statutes),

we will comply with the applicable timeline. Notification will include a description of the incident, the categories of data affected, and steps we are taking to address the breach.

13. Cookies

We use only essential cookies necessary to operate the service. All cookies are set with httpOnly, secure, and SameSite=Lax flags.

- Teacher session cookie — maintains login session (expires after 14 days of inactivity or upon logout)
- Student session cookie — contains only an internal student identifier and class identifier (no student names or personal information). Expires after 4 hours. Not used for tracking across sessions or devices.
- Class code cookie — stores only the class code string so students can re-enter their class without re-typing the code. Expires after 14 days. Contains no student-identifying information.

We do not use advertising cookies, tracking cookies, or any cookies for analytics or profiling purposes.

14. Automated Decision-Making

We do not use personal data for profiling or automated decision-making that produces legal or similarly significant effects on individuals.

Reading-level adjustments are made to instructional content at the teacher's direction and do not constitute automated decision-making with legal or significant effects on students. AI-generated content adjustments are made available to teachers, who retain discretion over what materials are provided to students.

15. Data Portability

Schools and authorized users may request export of their data (including student rosters, assignments, and generated content) by contacting support@lift-off.me. We will fulfill data export requests within 30 days. Exported data will be provided in a commonly used, machine-readable format (e.g., CSV or JSON).

16. Business Transfers and Service Discontinuation

Transfer of Ownership

In the event that ownership of Lift Off is transferred to another person or entity, the new owner will be bound by the terms of this privacy policy with respect to all previously collected student and teacher data. If the new owner intends to materially change the handling of student data, affected schools will be notified at least 90 days in advance and given the opportunity to request deletion of all student data before any such transfer takes effect.

Discontinuation of Service

In the event that Lift Off ceases operations or discontinues the Lift Off service, we will provide schools and account holders with at least 90 days' written notice. During the notice period, schools may request export or deletion of all associated data. Upon expiration of the notice period, all remaining student data, teacher data, and educational content will be permanently deleted. Automated infrastructure backups will be destroyed within 7 days following final data deletion.

17. Audit Cooperation

We will reasonably cooperate with school or district audits related to data protection obligations under this policy or applicable law. Audit requests may be directed to support@lift-off.me.

18. Changes to This Policy

We may update this policy periodically to reflect changes in our practices or applicable law. Material changes will be communicated via email to the account holder and reflected with an updated effective date at the top of this policy.

Material changes to the handling of student data will require affirmative consent from the school or authorized account holder before taking effect. For all other material changes, continued use of the service after the effective date constitutes acceptance of the updated policy. If you do not agree to a material change, you may terminate your account and request deletion of your data.

19. Contact

For privacy-related questions, data access requests, data export requests, or to request a Data Processing Agreement, please contact:

Lift Off

Operated by Andrew Atkins and Morgan Atkins

3814 Arnold Ave, Apt 1, San Diego, CA 92104

support@lift-off.me