RapidBubble Security Overview

RapidBubble is a web app teachers use to print bubble sheets, grade them from a copier scan or document camera, and send scores to the district's LMS. It is used by teachers only: students never sign in, never create accounts and never enter anything into the app.

The app collects the minimum needed to grade a test and record the score: a bubbled student ID number, the answers on the sheet, the scan image, and the class roster (from the district's LMS, ClassLink or Google Classroom) for matching. It is a single-purpose service with no advertising, no student profiles and no sale of data, built and operated by a classroom teacher in California. We sign the Student Data Privacy Consortium's National Data Privacy Agreement.

WHAT DATA WE COLLECT

Student data enters RapidBubble two ways: the class roster (from the district's LMS, ClassLink, or a teacher's Google Classroom) and the bubble sheet itself. Everything else is teacher account data.

Data	Where it comes from	Why we hold it	Kept for
Student name, LMS user ID, SIS student ID, email	The class roster: LMS (LTI Names and Role Provisioning), ClassLink (OneRoster) or Google Classroom	Match each scanned sheet to the right student	Refreshed from its source; deleted at the district's request or end of agreement
Bubbled student ID and class period, answers read from the sheet, score	The scanned sheet	Grade the test and show results	2 years, then deleted automatically
Scan image of each sheet (grayscale JPEG, may show a handwritten name)	The copier PDF or camera frame	Let the teacher check flagged sheets	60 days, then deleted automatically
Scores sent to the gradebook (the LMS, Google Classroom, or the SIS through ClassLink) and when	Grade sync	Avoid re-sending unchanged scores	With the result
Teacher name, email, school, hashed password; LMS, Google, Microsoft or ClassLink account ID; encrypted Classroom token; how they found us	Signup, LTI launch, SSO sign-in or connecting Classroom	Sign the teacher in, scope sharing to their district, reach their classes	While the account is open (Classroom token: until disconnected, which revokes it)
Tests: titles, answer keys, questions, choices and pictures imported from Word or PDF	The teacher	Print versions and grade	Until the teacher deletes the test (the uploaded file itself is not kept)
Sheets graded per account per month	The app	Billing and usage reports; holds no student data	Indefinitely
Server logs: IP address, browser, pages requested	Web server	Security and troubleshooting	Standard log rotation

Never collected: student accounts, passwords, grades from other assignments, demographics, disability or discipline records, free-text student responses, device identifiers, location, or anything from students directly. No student data is ever used for advertising or to train AI models.

WHERE DATA LIVES AND HOW IT IS PROTECTED

All data is stored in the United States on a dedicated Linode (Akamai) server running Ubuntu 24.04, with a PostgreSQL database and scan images on the server's own disk. Nothing is stored on a laptop or in a consumer cloud account.

- **In transit:** HTTPS everywhere. Traffic passes through Cloudflare in "Full (strict)" mode: encrypted from the browser to Cloudflare and again from Cloudflare to our server's own certificate. HTTP Strict Transport Security is on, and sign-in and form cookies are marked Secure and SameSite.
- **Scan images** are never served as plain files by the web server. Every image is served through the app, which checks that the requester is the teacher who scanned it.
- **Passwords** are stored only as salted PBKDF2-SHA256 hashes. Teachers who sign in through the LMS, Google, Microsoft or ClassLink have no password with us at all.
- **Secrets** (database credentials, signing keys, OAuth secrets) live in a file readable only by the service account, never in source control. The LTI signing key is a 2048-bit RSA key.
- **Dependencies** are pinned to specific versions, and front-end libraries are self-hosted, so app pages make no requests to third-party servers.
- **At rest:** the server's disks use Linode's platform-managed disk encryption. The server has no unencrypted storage volumes.
- **Backups:** Linode's Backup Service takes automatic daily snapshots of the server, kept in the same US data center and rotated within about two weeks, so deleted scan images don't linger in backups. The database is also backed up before every deploy. These snapshots are not encrypted at rest; we plan to move to encrypted database backups in a private storage bucket.

WHO CAN SEE WHAT

Access is checked on every page by the app, not by convention.

- **Tests** belong to the teacher who made them, who can share one (view, edit or re-share) only with colleagues verified in the same district.
- **Results and scan images** are visible only to the teacher who scanned them, except that on the district's common assessments, administrators it designates see results (not images) by school and teacher.
- **Rosters** are attached to a course only when the LMS, ClassLink or Google Classroom says the teacher teaches it, and are shown only to the test's owner and the course's teachers. A student who opens the LMS link is turned away.
- **Districts stay separate.** Every LMS registration has its own credentials, and a course is tied to the registration it was launched through, so one district's installation cannot read or write another's courses or grades. Classroom access is each teacher's own.
- **RapidBubble staff** reach the admin site only with a password plus an authenticator-app code, at an unpublished address. Staff access is limited to the operator and is used for support, setup and the usage reports, which contain no student data.

SIGN-IN AND AUTHENTICATION

District teachers normally never create a RapidBubble password: they open the app from the LMS, which signs them in.

Method	How it works
LMS launch (LTI 1.3)	The LMS sends a signed token; we verify its signature, issuer, audience, nonce and deployment before signing the teacher in. Only users with a teaching role get in.
Sign in with Google, Microsoft or ClassLink	OpenID Connect with PKCE. We verify the ID token's signature, issuer, audience, expiry and nonce. We never see the teacher's password with them and request no access to mail or files. ClassLink student and parent accounts are refused.
Password accounts	Django's password validators, hashed storage, and email confirmation of the address.
Lockout	10 failed sign-ins for a username from one address locks that pair for 15 minutes. Password reset is rate-limited per address and per email.
Staff admin	Password plus a time-based one-time code from an authenticator app, with one-use backup codes.
Sessions	Cookies are HTTPS-only and SameSite. Sessions expire after two weeks of inactivity, and signing out ends the session on the server.

RETENTION AND DELETION

Deletion is automatic and runs nightly. Nothing with student data is kept indefinitely.

Data	Deleted
Scan images	60 days after scanning (the score is kept)
Uploaded copier PDFs	As soon as grading finishes; an abandoned upload within 7 days
Graded results	730 days (2 years) after scanning
Class rosters	Replaced on each refresh; removed at the district's request or when the agreement ends
Tests and keys	When the teacher deletes them, or at the district's request
Teacher accounts	On request, or at the end of the agreement

A district can ask for its data to be returned or deleted at any time, including before an agreement ends. Deleting a result also deletes its image file.

THIRD PARTIES

These providers help run the service, and none receives student data as a product input.

Provider	Role · sees student data?
Linode (Akamai)	Server hosting, United States. Stored on their infrastructure under their data processing terms.
Cloudflare	TLS, DDoS protection and traffic proxy. Traffic passes through encrypted.
Google Workspace	Outgoing account email to teachers (password resets, confirmations). No student data.
Google Analytics	Visit counts on the public marketing pages only. Never loads after sign-in. Ad features off.
Anthropic	AI question checks (School & District plan): test questions and pictures only, no student data. Never used for training; deleted within 30 days (up to 2 years if flagged for a policy violation).

Kept on our server: uploaded tests are parsed and bubble sheets graded by our own code, with no outside OCR. App pages load no third-party scripts, fonts or trackers.

PRIVACY COMMITMENTS

Student data belongs to the school. We hold it as a school official under FERPA, use it only as the school directs, and give it back or delete it on request.

- **No advertising, no selling, no profiling.** Student data is never used for marketing, never sold or rented, and never used to train AI models.
- **COPPA:** students never use the app, so no data is collected from children directly.
- **California:** we comply with the Student Online Personal Information Protection Act (SOPIPA) and Education Code 49073.1, and sign the district's required agreement.
- **Agreements we sign:** the Student Data Privacy Consortium's National Data Privacy Agreement, including the California Student Privacy Alliance version; New York Education Law 2-d and Illinois SOPPA exhibits on request.
- **Breach notification:** if we learn of a breach affecting student or teacher data, we notify affected districts promptly, and no later than 72 hours after discovery, or sooner where the district's state law or agreement requires it.
- **Changes:** we never reduce protection for data already collected without the district's consent.

Contact. Security questions, data deletion requests and privacy agreements: support@rapidbubble.com. We answer security questionnaires (SDPC and HECVAT formats) and can walk your IT team through the LMS installation in about 30 minutes. Policy and Terms: rapidbubble.com/privacy · rapidbubble.com/terms