

LEGAL

Privacy policy

Effective September 17, 2026. This policy covers both this website and the BreathEasy I Campus™ application, and it applies to every district, school, and organization that uses the service.



WHAT THIS POLICY COVERS

- This website and the Campus application
- Every district, school, and organization we serve
- What we collect and why
- How long records are kept and how to reach us

Who we are

BreathEasy I Campus™ is operated by BreathEasy Administrative Services LLC, 201 Lupin Street, Pahrump, Nevada 89048. The company controls the hosting account for the application and database, and it is the entity that stores the data described here. Privacy questions go to help@breatheasy.net.

Our role under FERPA

When a school or district uses BreathEasy I Campus™, education records stay under the control of that education agency. The company acts as a school official with a legitimate educational interest under FERPA, 34 CFR 99.31(a)(1)(i)(B). That means we perform a service the agency would otherwise perform itself, we use education records only for that purpose

and only as the agency directs, and we do not re-disclose student information to anyone else except as the agency instructs or the law requires.

Districts and schools decide who at their organization may see which records. We provide the controls; the agency makes the decisions.

What the application collects

- Student roster information supplied by the school: name, grade, homeroom, badge or tag identifier, and guardian name and email.
- Records staff create: behavior tallies and timers, ABC incident notes, intervention and accommodation logs, IEP goal progress, daily report cards, hall passes, discipline referrals and statements, urgent incident records, roll call responses, bus ratings and tickets, and any photo or file a staff member attaches to a case.
- Staff account information: name, work email, title, school, and role.
- Technical records needed to run the service securely: sign-in events, administrative actions, records of each use of an AI drafting feature (who ran it, when, and the student record involved), and error logs.
- Approximate device location, only when a staff member submits an emergency roll call or a safety report where location is part of the report.
- Facial lookup reference images and mathematical face templates, only for districts that authorize and enable the optional facial lookup capability. The capability is disabled by default and appears only after a district enables it.

Students do not create accounts. The one student-facing surface, the statement kiosk used during a discipline investigation, collects only the statement the student writes.

Why we use it

Only to deliver the service the school contracted for: recording and reporting behavior and discipline, tracking progress toward goals, communicating with guardians, running campus safety workflows, supporting staff, and keeping the system secure and available. We do not sell student data. We do not use it for advertising or marketing. We do not use it to build profiles for any purpose outside the school's own use, and we do not use it to train unrelated systems or models.

Guardian communication

Report cards, discipline notices, and similar messages are sent to the guardian address the school provides, from the company's sending domain on the school's behalf. Guardian view links are read-only, scoped to a single student, and expire. Guardians who wish to stop

receiving messages, or who believe a record is wrong, should contact their school; the school controls the record.

Who else touches the data

A short list of sub-processors, each bound by contract and none permitted to use the data for their own purposes:

- Application hosting (Lovable), which serves the web application from Cloudflare’s global edge network with United States processing.
- Database, sign-in, and private file storage (Supabase), running on Amazon Web Services in the US East (Ohio) region. This is where student and staff records actually live.
- Transactional email (Lovable messaging), which delivers report cards, notices, and account email.

We do not own or operate data centers. The underlying infrastructure is Amazon Web Services and Cloudflare, reached through managed platforms, and all of it operates in United States regions on infrastructure certified to SOC 2 Type II and ISO 27001. The full table, including what each one touches, is in the [district addendum \(/district-addendum\)](#).

No advertising networks, data brokers, or social platforms receive any data from the application. We disclose information outside this list only with the district’s instruction or when required by law, and we tell the district first unless we are legally prohibited from doing so.

Where data is stored and how it is protected

The application, database, and file storage are hosted in United States cloud regions only. The database and files sit on Amazon Web Services in the US East (Ohio) region, us-east-2, and the application is served from Cloudflare’s edge network. We do not own data centers; both are major cloud providers reached through managed platforms. Data is encrypted in transit with TLS 1.2 or higher and at rest with AES-256. Access uses role checks and database-level policies to enforce school and district boundaries. Full detail is in the [data security and incident response policy \(/security\)](#), including our commitment to notify a district within 72 hours of confirming a breach involving their data.

How long we keep it

These are the defaults. A district may set different periods in its agreement.

Record type	Default retention

Student behavior, discipline, IEP progress, and report card records	Current school year plus 5 years
Urgent incident, restraint and seclusion, and mandated-reporter records	7 years, immutable
Hall passes, roll calls, and other operational logs	18 months
Staff accounts and sign-in logs	3 years after the account is deactivated
Cookie-free website measurement	25 months, aggregated
Website inquiry and demo request messages	24 months
Facial lookup reference templates, when enabled by written district authorization	District-defined; deleted when the option is disabled or upon written request

On written request, or when a contract ends, the district receives a full export, live data is permanently deleted within 30 days, and backup copies age out on the normal 35-day cycle.

Parent and student rights

Requests to inspect, correct, or delete a student record are handled by the school or district that holds the record, as FERPA requires. If a request reaches us directly, we forward it to the district and support them in responding. For students under 13, the school provides the consent contemplated by COPPA in its role as the parent's agent, and we collect nothing beyond what the school's educational purpose requires.

We honor state student-privacy laws generally, including restrictions on targeted advertising, profiling, and secondary use. Optional facial lookup is disabled by default and is configured only after written district authorization, confirmation of applicable legal requirements, and any required notice or consent. When enabled, live comparison occurs on the staff device, live camera frames are not retained, reference templates remain in restricted storage, and the district controls deletion.

This website

The public website uses no tracking cookies, no advertising pixels, and no third-party analytics, so no cookie banner is needed. We record anonymous page-view measurement: the page path, the time, the referring domain, a general device type, and a visitor hash that is derived without storing an IP address and rotates every day. That measurement cannot be tied back to a person, and staff-only pages are excluded.

If you send us a message through a form, we receive what you type: your name, email, phone if you provide it, organization, and your message. We use it to reply and to send information you

asked for. Marketing email includes a working unsubscribe link and our mailing address, and we honor opt-outs promptly. Please do not send student personal information through a website form.

District addendum

Some items are set per district rather than in this policy, because they belong in the signed agreement: the retention periods that district chooses, its authorized contacts for data requests and breach notification, which optional features are turned on, single sign-on configuration, and any state-specific addendum or NDPA exhibit the district requires. Those terms control where they differ from the defaults here.

Changes and contact

We update this policy as the product changes and note the effective date at the top. Material changes affecting student data are communicated to district contacts before they take effect.

BreathEasy Administrative Services LLC
201 Lupin Street, Pahrump, Nevada 89048
Privacy and support: help@breatheasy.net
Sales and contracts: sales@breatheasy.net

Document version

Privacy policy version 1.3, effective September 18, 2026. A current copy of this document, plus downloadable PDFs, are available at </district-documents/>.