FOR DISTRICTS

District addendum and schedule of data

Effective September 18, 2026. The line-item disclosures district counsel and technology directors ask for: exactly what we collect, exactly what we refuse to collect, who hosts it and where, and the state-specific terms that sit on top of our general policies.

WHAT THIS DOCUMENT ANSWERS

- Every data element we store, line by line
- The data we will not accept
- Named hosting providers and regions
- State-specific and deployment terms

How to use this document

This addendum supplements the privacy policy (/privacy) and the data security and incident response policy (/security). Those two documents are written to apply to any district in any state. This one holds the items that change by district or by state: the data inventory, the named sub-processors, the questionnaire offer, deployment terms, and the Nevada-specific addendum. Where a signed agreement differs from anything here, the signed agreement controls.

Data minimization: what we do not collect

The standard roster is limited to the fields used by the service: student name, grade, section, and a school-assigned identifier. We do not request, do not need, and will not accept the following.

- Social Security numbers or any government identification number.
- Health, medical, immunization, or mental-health treatment records.
- Free and reduced-price lunch status, or any other socioeconomic indicator.
- Financial account, payment card, or billing information for students or families.
- Fingerprints and voiceprints. Facial lookup reference images and mathematical face templates are collected only when a district authorizes and enables the optional facial lookup capability, which is disabled by default.
- Disciplinary or academic history imported from another system. Discipline records in the product are only the ones your own staff create inside it.
- Student home addresses, family immigration status, religious affiliation, or juvenile justice records.
- Precise or continuous location tracking of students. Device location is captured only from the staff member's device at the moment they submit an emergency roll call or a safety report.
- Anything used for advertising, marketing, resale, data brokerage, or training systems unrelated to your school's own use.

If a roster file you send happens to contain any of these fields, we drop them on import rather than store them, and we tell you which columns were discarded.

Schedule of data

Every data element the application stores, what it is for, and how long it is kept. Districts use this as the line-item checklist an NDPA Exhibit B expects. Anything not listed here is not collected, and we will not begin collecting a new category without telling you first and amending this schedule.

Category	Data elements	Source	Purpose	Default retention
Student identity	Legal or preferred name, grade, homeroom or section, school-assigned student ID, optional badge or NFC tag identifier	District roster import (CSV) or staff entry	Identify the correct student when staff log an event	School year plus 5 years
Guardian contact	Guardian name and email address	District roster import or staff entry	Deliver report cards and discipline notices the school authorizes	School year plus 5 years

Behavior and intervention records	Behavior tallies, duration timers, ABC incident notes, intervention logs, accommodation delivery logs, check-in / check-out point sheets, fidelity logs	Staff entry during the school day	Tier 2 and Tier 3 progress monitoring and MTSS decision making	School year plus 5 years
IEP goal progress	Goal text authored by school staff, measurement type, progress data points	Staff entry	Progress reporting toward goals the district already writes	School year plus 5 years
Discipline records	Referral details, infraction, location, period, severity, witness and student statements, resolution, attached photos or files	Staff entry and the student statement kiosk	Office investigation, resolution, guardian notification, and SIS export	School year plus 5 years
Urgent incident records	Restraint, seclusion, elopement, and medical event timelines, follow-up reports, cancellation reasons, mandated-reporter records	Staff entry	Crisis documentation and state reporting obligations	7 years, immutable
Campus operations	Hall passes, emergency roll call responses, campus alerts and drills, after-school check-ins, staff hub submissions	Staff entry	Tier 1 campus safety and supervision	18 months
Transportation	Per-run bus ride rating (green, yellow, red) and bus referral tickets	Driver or transportation staff entry	Bus behavior tracking and transportation follow-up	School year plus 5 years
Staff accounts	Name, work email, job title, assigned school, assigned roles	District IT administrator	Authentication and permission enforcement	3 years after deactivation

Security and audit logs	Sign-in successes and failures, password resets, role changes, exports, support access, administrative actions, IP address, user agent, timestamp	Generated automatically by the system	Security monitoring, breach detection, and district audit review	18 months
Device location	Approximate device location at the moment of submission only	Staff device, with explicit browser permission	Locate staff and students during an emergency roll call or safety report	18 months, with the parent record
Optional facial lookup	Reference images and mathematical face templates; live camera frames are not retained	District-authorized enrollment by restricted staff; disabled by default	Camera-assisted student lookup on an authorized staff device	District-defined; deleted when the option is disabled or upon written request
Website measurement	Page path, timestamp, referring domain, general device type, daily-rotating visitor hash. No cookies, no IP storage, no student data	Public marketing website only	Aggregate traffic measurement	25 months, aggregated

Students do not hold accounts. The only student-facing surfaces are the discipline statement kiosk, which captures only the statement the student types, and the read-only family view, which displays records the school already created.

Hosting and sub-processors

BreathEasy Administrative Services LLC does not own or operate data centers, servers, or network hardware. The service runs on two major cloud providers, Amazon Web Services and Cloudflare, reached through managed platforms that provision, patch, and monitor those resources on our behalf. Below is the full named list of every third party that touches district data, what each one handles, and where it physically sits.

Sub-processor	Role	Data it touches	Region	Compliance posture

Application hosting (Lovable, managed platform)	Serves the web application and server functions, with all data processing bound to United States regions	Request data in transit; no persistent student records stored at this layer	Cloudflare global edge network, United States processing	Cloudflare data centers hold SOC 2 Type II and ISO 27001
Database, authentication, file storage (Supabase, managed platform)	Managed PostgreSQL database, authentication, and private file storage for referral photos and attachments	All student, staff, discipline, and audit records	Amazon Web Services, US East (Ohio), us-east-2	Supabase holds SOC 2 Type II; AWS data centers hold SOC 2 Type II and ISO 27001
Transactional email (Lovable messaging, managed platform)	Delivers report cards, discipline notices, account emails, and security alerts	Recipient email address and message contents only	United States	Operates on SOC 2 Type II certified infrastructure

Provider certifications apply to the infrastructure controls and services identified in those reports. BreathEasy is responsible for application design, access rules, role assignment, data handling, tenant separation, support access, and the policies governing use of the service.

No advertising networks, analytics vendors, data brokers, or social platforms receive any data from the application. Each sub-processor is bound by terms at least as restrictive as our agreement with your district, and none may use district data for its own purposes. We notify district contacts before adding or replacing a sub-processor that handles student data.

Independent attestations and self-assessment

BreathEasy Administrative Services LLC does not currently hold its own SOC 2 report. The following supporting information is available for district review.

- Provider assurance: the underlying data centers, physical storage, and network infrastructure operate within environments holding SOC 2 Type II and ISO 27001 certifications. Provider reports are available upon request and apply to the controls and services they cover.
- Self-assessment: completed Consensus Assessments Initiative Questionnaire (CAIQ) v4.1 and HECVAT 4.1.6 are included in the district packet, covering encryption, access control, authentication, backup and recovery, sub-processor management, and incident response.
- Documented controls: the security policy, privacy policy, sub-processor list, Schedule of Data, access-control summary, security logging summary, and incident-response terms are included in the district packet.

- Contract terms: audit rights and district-specific data protection terms are established in the signed district agreement.
- Insurance: cyber-risk and technology errors and omissions coverage is carried through Hiscox with a $250,000 aggregate limit, policy period through February 24, 2027. Certificates of insurance, including certificates naming the district, are issued on request.
- Penetration testing: an independent third-party penetration test of the application has not been performed. A gray-box test would cover application endpoints, authentication and session handling, role enforcement, and multi-tenant separation.
- Governance: the company has two members. One is the designated security officer and incident commander; the other is the designated privacy officer and backup incident commander.
- Network intrusion detection and prevention, host hardening, and configuration monitoring for the underlying infrastructure are provided by Cloudflare and Amazon Web Services under their certified programs. Application-level activity is covered by the security event log.

Download the completed questionnaires from /district-documents (/district-documents), individually or inside the complete packet ZIP. Questions about any answer: help@breatheasy.net.

Deployment scope

The written district agreement defines participating schools, programs, roles, enabled modules, data categories, duration, and authorized district contacts before district data is imported.

- Data use begins after the district authorizes the deployment scope in writing.
- Optional capabilities are enabled only when listed in the written district scope and configured during onboarding.
- The privacy, security, export, retention, and deletion terms apply to the authorized deployment scope.
- At contract end, the district receives a full export and live data is permanently deleted within 30 days unless the signed agreement states otherwise.

Breach cooperation and costs

Our general commitments on detection, notification timelines, and post-incident reporting are in the data security and incident response policy (/security). The following apply specifically to a confirmed breach originating on infrastructure we control.

- We notify the district's designated contact without unreasonable delay and no later than 72 hours after confirming the incident, with what happened, what data was involved, and what we are doing.

- We cooperate fully with the district's own notification duties under state breach-notification law and its contractual obligations, and we provide the factual detail the district needs to write its notices.
- We bear the reasonable cost of forensic investigation of our own systems, and of parent and staff notification and credit monitoring where those costs are attributable to a breach on our infrastructure. Final allocation is set in the signed agreement.
- We do not contact parents or students directly about an incident unless the district asks us to in writing.
- A written post-incident report covering root cause, remediation, and preventive changes follows within 15 business days.

State privacy addenda (Nevada included by default)

For Nevada districts, the following state-specific terms apply in addition to our general policies. They track the operator obligations in NRS 388.267 through 388.296, originally enacted as SB 463.

- No targeted advertising. We do not serve, and will not permit any third party to serve, behavioral or targeted advertising to students based on any information collected through the service.
- No commercial profiling. We do not build profiles of students for any purpose other than delivering the educational service the district authorized.
- No sale or rental of pupil records. Student data is never sold, leased, licensed, or transferred to data brokers, marketers, or any third party for commercial purposes.
- Deletion within 30 days. On written district request or at contract termination, we securely destroy or return all covered student information within 30 days, and we provide written certification that live records, cached copies, and backups have been purged or rendered permanently unrecoverable.
- District ownership. All student personally identifiable information remains the exclusive property of the local educational agency. We claim no intellectual property rights in uploaded or generated student records.
- School official designation. The district designates the service as a school official with a legitimate educational interest under 34 CFR 99.31(a)(1)(i)(B), which is what allows the district to share records with us without individual parental consent.
- Operators who violate these provisions are subject to civil penalties of up to $5,000 per violation under Nevada law. We accept those obligations contractually.

We serve districts nationwide. The general privacy and security policies are written to be state-neutral so that only this document changes from state to state. We provide the standard NDPA state-specific terms on request, including California (CSDA), Texas (TX-NDPA), Illinois (SOPPA), and New York (Education Law 2-d) addenda. Nevada terms ship by default because that is where the company is organized. Request your state's addendum from sales@breatheasy.net.

Contact

BreathEasy Administrative Services LLC
201 Lupin Street, Pahrump, Nevada 89048
Security, privacy, and questionnaires: help@breatheasy.net
Contracts and pilots: sales@breatheasy.net

Document version

District addendum and schedule of data version 1.4, effective September 18, 2026. A current copy of this document, plus downloadable PDFs, are available at /district-documents (/district-documents).