

BreathEasy | Campus™

BreathEasy Administrative Services LLC
201 Lupin Street, Pahrump, Nevada 89048
help@breatheasy.net | sales@breatheasy.net

September 18, 2026

To the reviewing technology director, special education director, or procurement officer:

This letter summarizes the product, privacy, security, hosting, and data-handling information contained in the attached policies and corresponding live pages.

1. Product overview and functional specification

BreathEasy | Campus™ is a single, browser-based web application for school climate, behavior, discipline, and crisis response across all three MTSS tiers. It is built for Windows and Chromebook districts: every staff workflow runs in a browser with nothing to install and no extension to approve. The one hardware-dependent feature is NFC tap-to-identify, which runs on rugged Android handhelds. Those handhelds can be enrolled and managed through the same UEM/MDM console the district already uses for Chromebooks (Google Admin, Microsoft Intune, VMware Workspace ONE, and similar). Every NFC screen also offers a manual student picker, so no task is blocked on a device without NFC.

Student-facing surfaces, including the discipline statement kiosk and the family portal, require only a standard browser tab: no camera, no NFC, and no special permissions.

Optional facial lookup is disabled by default at the district level and appears only after a district enables it. It is available as a district-specific implementation where authorized in writing and where applicable notice and consent requirements are satisfied. Live comparison occurs on the staff device, live camera frames are not retained, and reference data is restricted and district-controlled.

See: [BreathEasy-Campus-Product-Overview.pdf](#) and the live page at campus.breatheasy.net/product-overview.

2. Privacy policy, FERPA, and the entity storing the data

The service is operated by BreathEasy Administrative Services LLC, 201 Lupin Street, Pahrump, Nevada 89048. The company controls the hosting account and is the entity storing the data. Under FERPA the company acts as a school official with a legitimate educational interest, 34 CFR 99.31(a)(1)(i)(B), using student data only for the purpose the school directs and not re-disclosing it except as the school instructs or the law requires.

Student data is never sold, never used for advertising, and never used to train unrelated systems or models.

See: [BreathEasy-Campus-Privacy-Policy.pdf](#) and the live page at campus.breatheasy.net/privacy.

3. Data security and incident response

Data is encrypted in transit with TLS 1.2 or higher and at rest with AES-256. Access is least-privilege and uses database-level policies and application role checks to enforce school and district boundaries. Backups run daily on a 35-day rolling cycle with tested restore procedures. Sign-in attempts, account lockouts and unlocks, role changes, support access, and each use of an AI drafting feature are logged, an account locks after five failed sign-in attempts within ten minutes, staff sessions end automatically after 30 minutes with no activity, and district IT can review and export those events from the admin console.

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 naming the district are issued on request. An

independent third-party penetration test of the application has not been performed. The company has two members: one is the designated security officer and incident commander, the other the designated privacy officer and backup incident commander.

If a confirmed breach involving district data occurs, the district is notified no later than 72 hours after confirmation, with a written post-incident report within 15 business days. Report a suspected incident to help@breatheasy.net with "SECURITY" in the subject line.

See: [BreathEasy-Campus-Data-Security-and-Incident-Response.pdf](#) and the live page at campus.breatheasy.net/security.

4. Hosting, sub-processors, and attestations

The company does not own or operate data centers. The application runs on two major cloud providers, Amazon Web Services and Cloudflare, reached through managed platforms that provision and patch those resources on our behalf. All processing stays in United States regions:

- Web application and server functions: served from Cloudflare's global edge network through the Lovable managed platform, with processing bound to United States regions.
- Database, authentication, and private file storage: managed PostgreSQL through the Supabase platform, running on Amazon Web Services in the US East (Ohio) region, us-east-2. This is where student and staff records physically reside.
- Transactional email: a managed United States sending service delivers report cards, discipline notices, and account email.

Both layers sit on infrastructure covered by SOC 2 Type II and ISO 27001 programs, and those attestation reports are available on request. Those provider attestations apply to the controls and services covered by their reports. BreathEasy controls the application design, access rules, roles, data handling, tenant separation, policies, and support practices. The company does not currently hold its own SOC 2 report. Completed CAIQ v4.1 and HECVAT 4.1.6 self-assessments are included in this packet, each as a readable PDF and as the official spreadsheet form.

Named accounts, email and password, Google sign-in, role-based access, account lockout, and manual deprovisioning are the default identity controls. Google Workspace or Microsoft Entra ID integration using SAML/OIDC, identity-provider MFA enforcement, and automated account lifecycle integration are available upon district request and configured during onboarding where supported by the district environment.

5. Schedule of data and state-specific terms

The district addendum carries the line-item Schedule of Data an NDPA Exhibit B expects, the list of data categories excluded from standard collection (Social Security numbers, health records, free and reduced-price lunch status, and others), conditional facial lookup data, the full sub-processor table, deployment terms, breach cost cooperation, and the Nevada student privacy addendum tracking NRS 388.267 through 388.296. We serve districts nationwide; the standard NDPA state-specific terms for California (CSDA), Texas (TX-NDPA), Illinois (SOPPA), New York (Education Law 2-d), and other states are available on request.

See: [BreathEasy-Campus-District-Addendum.pdf](#) and the live page at campus.breatheasy.net/district-addendum.

Sincerely,

BreathEasy Administrative Services LLC
help@breatheasy.net