Higher Education Community Vendor Assessment Toolkit (HECVAT) 4.1.6 - Completed

BreathEasy | Campus | Effective September 18, 2026

Completed by BreathEasy Administrative Services LLC for BreathEasy | Campus. Answers describe the service as it operates on the effective date. Where a control is provided by an infrastructure provider, the answer says so.

Contact: help@breatheasy.net

The official HECVAT 4.1.6 workbook with these same answers is included in the district packet.

START HERE

GNRL-01
Solution Provider Name
Answer: BreathEasy Administrative Services LLC

GNRL-02
Solution Name
Answer: BreathEasy | Campus™

GNRL-03
Solution Description
Answer: Web-based MTSS behavior, discipline, and campus safety platform for K-12 districts: NFC student lookup on staff handhelds, behavior tallies and timers, ABC incident notes, Tier 2/Tier 3 intervention and IEP goal progress tracking, discipline referrals with a student statement kiosk, urgent incident documentation, hall passes, emergency roll call, transportation ratings, and guardian report delivery.

GNRL-04
Solution Provider Contact Name
Answer: Customer Support

GNRL-05
Solution Provider Contact Title
Answer: Support and security contact

GNRL-06
Solution Provider Contact Email
Answer: help@breatheasy.net

GNRL-07
Solution Provider Contact Phone Number
Answer: Not published; all support is handled by email at help@breatheasy.net

GNRL-08
Country of Company Headquarters
Answer: United States

GNRL-09
Employee Work Locations (all)
Answer: United States (fully remote)

COMP-01
Do you have a dedicated software and system development team(s) (e.g., customer support, implementation, product management, etc.)?*

Answer: Yes

A small, dedicated team designs, develops, and supports the product. BreathEasy Administrative Services LLC is a two-member company. Both members perform operational duties. One member is designated security officer and incident commander; the other is designated privacy officer and backup incident commander, so incident response and district contact do not depend on one person.

COMP-02
Describe your organization’s business background and ownership structure, including all parent and subsidiary relationships.

Answer: BreathEasy Administrative Services LLC is a privately held Nevada limited liability company headquartered in Pahrump, Nevada. It has no parent company and no subsidiaries.

COMP-03
Have you operated without unplanned disruptions to this solution in the past 12 months?

Answer: Yes

No unplanned service disruptions affecting districts in the past 12 months.

COMP-04
Do you have a dedicated information security staff or office?

Answer: Yes

One company member is the designated security officer and incident commander; the other is the designated privacy officer and backup incident commander. Both review the security policy at least annually.

COMP-05
Use this area to share information about your environment that will assist those who are assessing your company's data security program.

Answer: The service is a managed cloud application: the web application is served from Cloudflare's edge network, and the database, authentication, and file storage run on managed PostgreSQL on AWS us-east-2. District tenancy is enforced at the database layer. Full details are in the published data security and incident response policy and district addendum at campus.breatheasy.net/district-documents.

REQU-01
Are you offering a cloud-based product?

Answer: Yes

REQU-02
Does your product or service have an interface?

Answer: Yes

REQU-03
Are you providing consulting services?

Answer: No

REQU-04
Does your solution have AI features, or are there plans to implement AI features in the next 12 months?

Answer: Yes

Limited AI-assisted drafting features (for example, suggested accommodation text). No district data is used to train AI models. See the AI tab.

REQU-05
Does your solution process protected health information (PHI) or any data covered by the Health Insurance Portability and Accountability Act (HIPAA)?

Answer: No

REQU-06
Is the solution designed to process, store, or transmit credit card information?

Answer: No

REQU-07
Does operating your solution require the institution to operate a physical or virtual appliance in their own environment or to provide inbound firewall exceptions to allow your employees to remotely administer systems in the institution's environment?

Answer: No

REQU-08
Does your solution have access to personal or institutional data?

Answer: Yes

Student and staff records supplied or created by the district, as itemized in the published Schedule of Data.

Organization

DOCU-01
Do you have a well-documented business continuity plan (BCP), with a clear owner, that is tested annually?*

Answer: Yes

Business continuity commitments (RTO 24 hours, RPO 24 hours, daily backups with point-in-time recovery) are documented in the security policy. BreathEasy Administrative Services LLC is a two-member company. Both members perform operational duties. One member is designated security officer and incident commander; the other is designated privacy officer and backup incident commander, so incident response and district contact do not depend on one person.

DOCU-02
Do you have a well-documented disaster recovery plan (DRP), with a clear owner, that is tested annually?*

Answer: Yes

Restore procedures are tested at least annually; backups are retained on a rolling 35-day cycle.

DOCU-03
Have you undergone a SSAE 18/SOC 2 audit?

Answer: No

BreathEasy Administrative Services LLC does not currently hold its own SOC 2 report. Underlying infrastructure (AWS, Cloudflare) operates under SOC 2 Type II and ISO 27001 certifications; provider reports are available on request. This completed questionnaire, the published security policy, and the named sub-processor list are provided for review.

DOCU-04
Do you conform with a specific industry standard security framework (e.g., NIST Cybersecurity Framework, CIS Controls, ISO 27001, etc.)?

Answer: Yes

Controls are organized consistently with the NIST Cybersecurity Framework functions and CSA Cloud Controls Matrix domains (this CAIQ/HECVAT submission). No formal certification is held.

DOCU-05
Can you provide overall system and/or application architecture diagrams, including a full description of the data flow for all components of the system?

Answer: Yes

Architecture and data flow are described in the product overview, security policy, and district addendum (named sub-processors, regions, and what each touches). Architecture diagrams are available to districts on request.

DOCU-06
Does your organization have a data privacy policy?

Answer: Yes

Published at campus.breatheasy.net/privacy and included in the district packet.

DOCU-07
Do you have a documented, and currently implemented, employee onboarding and offboarding policy?

Answer: Yes

Documented onboarding/offboarding: background checks and signed confidentiality agreements before production access, same-day revocation when a role ends.

THRD-01
Do you perform security assessments of third-party companies with which you share data (e.g., hosting providers, cloud services, PaaS, IaaS, SaaS)?*

Answer: Yes

Sub-processors are reviewed for security and privacy posture before use and are limited to the three named in the district addendum (application hosting, database/authentication/storage, transactional email).

THRD-02
Do you have contractual language in place with third parties governing access to institutional data?*

Answer: Yes

Each sub-processor is bound by terms at least as restrictive as the district agreement, and none may use district data for its own purposes.

THRD-03
Do the contracts in place with these third parties address liability in the event of a data breach?*

Answer: Yes

Provider terms address breach responsibility; breach cooperation and cost terms for the company itself are stated in the district addendum and set finally in the signed agreement.

THRD-04
Do you have an implemented third-party management strategy?*

Answer: Yes

A named sub-processor inventory is maintained in the district addendum, and districts are notified before a change affecting student data.

THRD-05
Do you have a process and implemented procedures for managing your hardware supply chain (e.g., telecommunications equipment, export licensing, computing devices)?

Answer: N/A

No company hardware supply chain; staff handhelds are district-owned devices managed through the district's MDM.

CHNG-01
Will the institution be notified of major changes to your environment that could impact the institution's security posture?*

Answer: Yes

Material changes affecting student data or security posture are communicated to district contacts before they take effect.

CHNG-02
Does the system support client customizations from one release to another?*

Answer: Yes

District configuration (roles, lists, schedules) persists across releases.

CHNG-03
Do you have an implemented system configuration management process (e.g., secure "gold" images, etc.)?*

Answer: Yes

Infrastructure is provisioned and patched by the managed platforms; application configuration is version controlled.

CHNG-04
Do you have a documented change management process?

Answer: Yes

All changes ship through version control with release-preparation review.

CHNG-05
Does your change management process minimally include authorization, impact analysis, testing, and validation before moving changes to production?

Answer: Yes

Changes pass build, type checking, and rendered verification before deployment.

CHNG-06
Does your change management process verify that all required third-party libraries and dependencies are still supported with each major change?

Answer: Yes

Dependency support and vulnerability status are checked during release preparation.

CHNG-07
Do you have policy and procedure, currently implemented, managing how critical patches are applied to all systems and applications?

Answer: Yes

Platform-level patching is handled by the managed platforms; application dependency updates are applied during release preparation.

CHNG-08
Have you implemented policies and procedures that guide how security risks are mitigated until patches can be applied?

Answer: Yes

Known high-severity vulnerabilities are evaluated and resolved before affected changes are deployed.

CHNG-09
Do clients have the option to not participate in or postpone an upgrade to a new release?

Answer: No

The service is continuously deployed SaaS; all districts run the current version. Security-affecting changes are announced.

CHNG-10
Do you have a fully implemented solution support strategy that defines how many concurrent versions you support?

Answer: Yes

A single current version is supported for all districts.

CHNG-11
Do you have a release schedule for product updates?

Answer: No

Updates are continuous rather than on a fixed schedule.

CHNG-12
Do you have a technology roadmap, for at least the next two years, for enhancements and bug fixes for the solution being assessed?

Answer: No

A published two-year roadmap is not provided; planned work is discussed with district contacts.

CHNG-13
Can solution updates be completed without institutional involvement (i.e., technically or organizationally)?

Answer: Yes

Updates deploy without district involvement.

CHNG-14
Are upgrades or system changes installed during off-peak hours or in a manner that does not impact the customer?

Answer: Yes

Deployments are zero-downtime edge releases.

CHNG-15

Do procedures exist to provide that emergency changes are documented and authorized (including after-the-fact approval)?

Answer: Yes

Emergency fixes follow the same version-controlled path and are reviewed after the fact.

CHNG-16

Do you have a systems management and configuration strategy that encompasses servers, appliances, cloud services, applications, and mobile devices (company and employee owned)?

Answer: Yes

Servers and cloud services are managed by the platforms; company endpoints are managed by the two company members; district devices remain district-managed.

PPPR-01

Do you have a documented patch management process?*

Answer: Yes

Patching of infrastructure is performed by the managed platforms; application dependencies are reviewed during release preparation.

PPPR-02

Can your organization comply with institutional policies on privacy and data protection with regard to users of institutional systems, if required?*

Answer: Yes

District policies are incorporated through the written district agreement and deployment scope.

PPPR-03

Is your company subject to the institution's geographic region's laws and regulations?*

Answer: Yes

The company operates under United States and state law, including state student-privacy statutes addressed in the district addendum.

PPPR-04

Can you accommodate encryption requirements using open standards?

Answer: Yes

TLS 1.2+ and AES-256 are open standards.

PPPR-05

Do you have a documented systems development life cycle (SDLC)?

Answer: Yes

Version-controlled development with release-preparation review and verification.

PPPR-06

Do you perform background screenings or multi-state background checks on all employees prior to their first day of work?

Answer: Yes

Background checks are completed before any access to production systems.

PPPR-07

Do you require new employees to fill out agreements and review policies?

Answer: Yes

Signed confidentiality and data-handling agreements are required.

PPPR-08

Do you have a documented information security policy?

Answer: Yes

Published in the district packet: data security and incident response policy.

PPPR-09

Are information security principles designed into the product lifecycle?

Answer: Yes

Least privilege, server-side enforcement, and data minimization are designed into the product.

PPPR-10

Will you comply with applicable breach notification laws?

Answer: Yes

Districts are notified no later than 72 hours after a confirmed breach involving their data.

PPPR-11

Do you have an information security awareness program?

Answer: Yes

Annual security awareness and FERPA training.

PPPR-12

Is security awareness training mandatory for all employees?

Answer: Yes

PPPR-13

Do you have process and procedure(s) documented, and currently followed, that require a review and update of the access list(s) for privileged accounts?

Answer: Yes

The company reviews its own access quarterly and on every personnel change; districts are asked to review staff accounts each semester.

PPPR-14

Do you have documented, and currently implemented, internal audit processes and procedures?

Answer: Yes

Internal review of security events, access lists, and policy conformance is performed by the security officer.

PPPR-15

Does your organization have physical security controls and policies in place?

Answer: Yes

No company data centers or on-premise servers; physical security of infrastructure is provider-operated under SOC 2 Type II / ISO 27001.

Product

AAAI-01

Does your solution support single sign-on (SSO) protocols for user and administrator authentication?*

Answer: Yes

Available upon district request and configured during onboarding: Google Workspace or Microsoft Entra ID via SAML or OIDC.

AAAI-02

For customers not using SSO, does your solution support local authentication protocols for user and administrator authentication?*

Answer: Yes

Default access uses named staff accounts with email and password or Google sign-in.

AAAI-03

For customers not using SSO, can you enforce password/passphrase complexity requirements (provided by the institution)?*

Answer: No

Standard password requirements are enforced (including screening against known breached passwords); district-defined custom complexity rules are not currently configurable for local accounts. Districts requiring specific policies use district SSO, where the

identity provider enforces them.

AAAI-04
For customers not using SSO, does the system have password complexity or length limitations and/or restrictions?*

Answer: Yes
Minimum length and leaked-password screening are enforced.

AAAI-05
For customers not using SSO, do you have documented password/passphrase reset procedures that are currently implemented in the system and/or customer support?*

Answer: Yes
Self-service password reset by email is implemented, with current-password confirmation required for authenticated password changes.

AAAI-06
Does your organization participate in InCommon or another eduGAIN-affiliated trust federation?*

Answer: No

AAAI-07
Are there any passwords/passphrases hard-coded into your systems or solutions?*

Answer: No
No hard-coded passwords; secrets are held in managed secret storage.

AAAI-08
Are you storing any passwords in plaintext?*

Answer: No
Passwords are stored only as salted hashes by the managed authentication service.

AAAI-09
Are audit logs available that include AT LEAST all of the following: login, logout, actions performed, and source IP address?*

Answer: Yes
Security events include sign-in successes and failures, lockouts and unlocks, role changes, support access, and AI drafting use, with timestamp, IP address, and user agent. District IT reviews and exports them from the admin console.

AAAI-10
Describe or provide a reference to the (a) system capability to log security/authorization changes, as well as user and administrator security events (i.e., physical or electronic), such as login failures, access denied, changes accepted; and (b) all requirements necessary to implement logging and monitoring on the system. Include (c) information about SIEM/log collector usage.*

Answer: The application logs sign-in attempts, account lockouts/unlocks, role changes, and support access with timestamp, actor, IP address, and user agent. Accounts lock automatically after five failed sign-ins within ten minutes and an alert is emailed to the district security/IT contact. District IT admins access logs in the admin console Security panel with export. No SIEM integration is required; logs can be exported for import into a district SIEM.

AAAI-11
Can you provide the institution documentation regarding the retention period for those logs, how logs are protected, and whether they are accessible to the customer (and if so, how)?*

Answer: Yes
Security event logs are retained 18 months, protected by row-level security (district IT and platform owner only), and viewable/exportable by district IT in the admin console.

AAAI-12
For customers not using SSO, does your application support integration with other authentication and authorization systems?

Answer: Yes

Google sign-in is standard; SAML/OIDC against the district identity provider is available upon request.

AAAI-13

Do you allow the customer to specify attribute mappings for any needed information beyond a user identifier? (e.g., Reference eduPerson, ePPA/ePPN/ePE)

Answer: No

Attribute mapping beyond the user identifier is not currently configurable.

AAAI-14

For customers not using SSO, does your application support directory integration for user accounts?

Answer: Yes

Automated account lifecycle integration is available upon district request where supported by the district's identity environment; manual same-day deprovisioning by the district admin is the default.

AAAI-15

Does your solution support any of the following web SSO standards: SAML2 (with redirect flow), OIDC, CAS, or other?

Answer: Yes

SAML2 and OIDC configurations are available upon district request during onboarding.

AAAI-16

Do you support differentiation between email address and user identifier?

Answer: Yes

Internal user identifiers are distinct from email addresses.

AAAI-17

For customers not using SSO, does your application and/or user frontend/portal support multifactor authentication (e.g., Duo, Google Authenticator, OTP, etc.)?

Answer: Yes

Google sign-in inherits the district's Google MFA policy; with district SSO, MFA policy is enforced by the district identity provider.

AAAI-18

Does your application automatically lock the session or log out an account after a period of inactivity?

Answer: Yes

Staff sessions end automatically after 30 minutes with no activity on both web and handheld clients, with an on-screen warning about one minute before sign-out. Accounts also lock after repeated failed sign-in attempts and can be deactivated by district administrators at any time.

DATA-01

Will the institution's data be stored on any devices (database servers, file servers, SAN, NAS, etc.) configured with non-RFC 1918/4193 (i.e., publicly routable) IP addresses?*

Answer: No

Database and storage are private and reachable only through the managed platform; no publicly routable database endpoints.

DATA-02

Is the transport of sensitive data encrypted using security protocols/algorithms (e.g., system-to-client)?*

Answer: Yes

TLS 1.2 or higher for every connection; HTTP redirects to HTTPS.

DATA-03

Is the storage of sensitive data encrypted using security protocols/algorithms (e.g., disk encryption, at-rest, files, and within a running database)?*

Answer: Yes

AES-256 encryption at rest for the database, backups, and uploaded files.

DATA-04

Do all cryptographic modules in use in your solution conform to the Federal Information Processing Standards (FIPS PUB 140-2 or 140-3)?*

Answer: Yes

Encryption is provided by AWS and Cloudflare managed services using FIPS 140-2 validated cryptographic modules.

DATA-05

Will the institution's data be available within the system for a period of time at the completion of this contract?*

Answer: Yes

At contract end the district receives a full export before deletion.

DATA-06

Are ownership rights to all data, inputs, outputs, and metadata retained even through a provider acquisition or bankruptcy event?*

Answer: Yes

District data remains district property; this survives acquisition or bankruptcy per the district agreement.

DATA-07

Do backups containing the institution's data ever leave the institution's data zone either physically or via network routing?*

Answer: No

Backups remain within the United States cloud regions operated by the providers.

DATA-08

Is media used for long-term retention of business data and archival purposes stored in a secure, environmentally protected area?*

Answer: Yes

Backup media is provider-managed in SOC 2 Type II / ISO 27001 certified data centers.

DATA-09

At the completion of this contract, will data be returned to the institution and/or deleted from all your systems and archives?

Answer: Yes

Full export on request; live data permanently deleted within 30 days; backups age out on the 35-day cycle; deletion confirmed in writing.

DATA-10

Can the institution extract a full or partial backup of data?

Answer: Yes

Districts may request a full or partial export at any time.

DATA-11

Do current backups include all operating system software, utilities, security software, application software, and data files necessary for recovery?

Answer: Yes

Provider-managed backups include everything required for full service restoration (point-in-time recovery).

DATA-12

Are you performing off-site backups (i.e., digitally moved off site)?

Answer: Yes

Backups are stored within the providers' US cloud infrastructure, separate from primary systems.

DATA-13

Are physical backups taken off-site (i.e., physically moved off site)?

Answer: No

No physical backup media is transported.

DATA-14

Are data backups encrypted?

Answer: Yes

AES-256 at rest.

DATA-15

Do you have a media handling process that is documented and currently implemented that meets established business needs and regulatory requirements, including end-of-life, repurposing, and data-sanitization procedures?

Answer: Yes

Media handling, end-of-life, and sanitization are operated by AWS and Cloudflare under their certification programs.

DATA-16

Does the process described in DATA-15 adhere to DoD 5220.22-M and/or NIST SP 800-88 standards?

Answer: Yes

Provider media sanitization follows NIST SP 800-88 guidelines.

DATA-17

Does your staff (or third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?

Answer: Yes

Named company personnel may access district data only for support and maintenance; access is logged and reviewable.

DATA-18

Do you have a documented and currently implemented strategy for securing employee workstations when they work remotely (i.e., not in a trusted computing environment)?

Answer: Yes

District data is accessed only through the browser; it is not stored on company workstations.

DATA-19

Does the environment provide for dedicated single-tenant capabilities? If not, describe how your solution or environment separates data from different customers (e.g., logically, physically, single tenancy, multi-tenancy).

Answer: Multi-tenant with logical separation: every district's records are isolated by row-level security policies enforced by the database itself, in addition to application-layer role checks.

DATA-20

Are ownership rights to all data, inputs, outputs, and metadata retained by the institution?

Answer: Yes

All student and district data remains the exclusive property of the district.

DATA-21

In the event of imminent bankruptcy, closing of business, or retirement of service, will you provide 90 days for customers to get their data out of the system and migrate applications?

Answer: Yes

Districts receive a full export window and cooperation for migration; 90 days can be committed in the agreement.

DATA-22

Are involatile backup copies made according to predefined schedules and securely stored and protected?

Answer: Yes

Automated daily backups with point-in-time recovery, encrypted, on a 35-day cycle.

DATA-23

Do you have a cryptographic key management process (generation, exchange, storage, safeguards, use, vetting, and replacement) that is documented and currently implemented, for all system components (e.g., database, system, web, etc.)?

Answer: Yes

Application secrets are held in managed secret storage; infrastructure keys are managed by the providers' key management services with rotation.

Infrastructure

APPL-01
Are access controls for institutional accounts based on structured rules, such as role-based access control (RBAC), attribute-based access control (ABAC), or policy-based access control (PBAC)?*

Answer: Yes
Role-based access control with district-defined roles, enforced at the database layer (row-level security) and re-checked on the server.

APPL-02
Are you using a web application firewall (WAF)?*

Answer: Yes
Cloudflare edge network provides web application firewall and DDoS protection in front of the application.

APPL-03
Are only currently supported operating system(s), software, and libraries leveraged by the system(s)/application(s) that will have access to institution's data?*

Answer: Yes
The application runs on currently supported, managed platforms; dependencies are reviewed during release preparation.

APPL-04
Does your application require access to location or GPS data?*

Answer: Yes
Approximate device location is captured only from a staff device, with explicit browser permission, at the moment an emergency roll call or safety report is submitted. No continuous or student location tracking.

APPL-05
Does your application provide separation of duties between security administration, system administration, and standard user functions?*

Answer: Yes
Distinct roles (teacher, office staff, administrator, IT admin, district admin, transportation) separate daily use from administration; company support access is separate, named, and logged.

APPL-06
Do you subject your code to static code analysis and/or static application security testing prior to release?*

Answer: Yes
Static type checking and security review are part of release preparation; known high-severity issues are resolved before affected changes deploy.

APPL-07
Do you have software testing processes (dynamic or static) that are established and followed?*

Answer: Yes
Changes pass type checking, production build, and rendered verification of affected screens before release.

APPL-08
Are access controls for staff within your organization based on structured rules, such as RBAC, ABAC, or PBAC?

Answer: Yes
Company access to production is limited to named personnel, used only for support and maintenance, and logged.

APPL-09
Does the system provide data input validation and error messages?

Answer: Yes
All input is validated on the server; privileged actions are re-checked server-side.

APPL-10

Do you have a process and implemented procedures for managing your software supply chain (e.g., libraries, repositories, frameworks, etc.)?

Answer: Yes

Dependencies are pinned in the project manifest and reviewed for known vulnerabilities during release preparation.

APPL-11

Have your developers been trained in secure coding techniques?

Answer: Yes

Secure coding expectations (server-side validation, least privilege, parameterized queries) are standard practice.

APPL-12

Was your application developed using secure coding techniques?

Answer: Yes

The application enforces parameterized database access, server-side authorization, and output encoding by framework default.

APPL-13

If mobile, is the application available from a trusted source (e.g., App Store, Google Play Store)?

Answer: N/A

The product is an installable web application (PWA); districts deploy it to managed handhelds and Chromebooks through their own MDM, not a public app store listing.

APPL-14

Do you have a fully implemented policy or procedure that details how your employees obtain administrator access to institutional instance of the application?

Answer: Yes

Company administrative access is limited to named personnel, granted only for support and maintenance, and recorded in the support access log.

DCTR-01

Select your hosting option.

Answer: Hybrid/Other

Managed cloud platforms: application delivery on Cloudflare's edge network; database, authentication, and storage on AWS us-east-2. All processing in United States regions.

DCTR-02

Is a SOC 2 Type 2 report available for the hosting environment?

Answer: Yes

SOC 2 Type II reports for the hosting environments (AWS, Cloudflare) are available to districts on request.

DCTR-03

Are you generally able to accommodate storing each institution's data within its geographic region?

Answer: Yes

All district data is stored and processed in United States regions only.

DCTR-04

Are the data centers staffed 24 hours a day, seven days a week (i.e., 24 x 7 x 365)?

Answer: Yes

Provider data centers are staffed 24x7x365.

DCTR-05

Are your servers separated from other companies via a physical barrier, such as a cage or hard walls?

Answer: Yes

Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

DCTR-06

Does a physical barrier fully enclose the physical space, preventing unauthorized physical contact with any of your devices?*

Answer: Yes

Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

DCTR-07

Are your primary and secondary data centers geographically diverse?

Answer: Yes

Providers operate geographically diverse facilities; the database region supports multi-zone availability.

DCTR-08

Is the service hosted in a high-availability environment?

Answer: Yes

The application is served from Cloudflare's globally redundant edge; the database runs on managed, monitored infrastructure with automated backups.

DCTR-09

Is redundant power available for all data centers where institutional data will reside?

Answer: Yes

Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

DCTR-10

Are redundant power strategies tested?*

Answer: Yes

Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

DCTR-11

Does the center where the data will reside have cooling and fire-suppression systems that are active and regularly tested?

Answer: Yes

Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

DCTR-12

Do you have Internet Service Provider (ISP) redundancy?

Answer: Yes

Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

DCTR-13

Does every data center where the institution's data will reside have multiple telephone company or network provider entrances to the facility?

Answer: Yes

Inherited from infrastructure providers. The application runs on managed platforms: Cloudflare's edge network (application delivery) and Amazon Web Services us-east-2 (database, authentication, file storage). Both providers hold SOC 2 Type II and ISO 27001 for the infrastructure they operate; their reports are available to districts on request.

DCTR-14

Do you require multifactor authentication for all administrative accounts in your environment?

Answer: Yes

Administrative access to hosting platforms requires MFA.

DCTR-15

Are you using your cloud provider's available hardening tools or pre-hardened images?

Answer: Yes

Managed platforms provision hardened, patched infrastructure on our behalf.

DCTR-16

Does your cloud solution provider have access to your encryption keys?

Answer: No

Application secrets are held in managed secret storage separate from provider-operated key material; providers cannot decrypt application secrets.

FIDP-01

Are you utilizing a stateful packet inspection (SPI) firewall?*

Answer: Yes

Cloudflare edge provides stateful inspection and managed WAF rules in front of the application.

FIDP-02

Do you have a documented policy for firewall change requests?*

Answer: Yes

Edge and firewall configuration changes are made through the managed platform under version-controlled deployment.

FIDP-03

Have you implemented an intrusion detection system (network-based)?*

Answer: Yes

Cloudflare provides network-level intrusion detection and DDoS mitigation.

FIDP-04

Do you employ host-based intrusion detection?*

Answer: No

Host-based intrusion detection is operated at the provider level, not separately by the company.

FIDP-05

Are audit logs available for all changes to the network, firewall, IDS, and IPS systems?*

Answer: Yes

Platform and network change logs are maintained by the managed platforms; application-level administrative changes are logged in the security event log.

FIDP-06

Is authority for firewall change approval documented? Please list approver names or titles in Additional Info.

Answer: Company members (security officer, with the second member as backup approver)

FIDP-07

Have you implemented an intrusion prevention system (network-based)?

Answer: Yes

Cloudflare managed WAF rules provide network-level intrusion prevention.

FIDP-08

Do you employ host-based intrusion prevention?

Answer: No

FIDP-09

Are you employing any next-generation persistent threat (NGPT) monitoring?

Answer: No

FIDP-10
Is intrusion monitoring performed internally or by a third-party service?
Answer: Third-party service (Cloudflare managed security)

FIDP-11
Do you monitor for intrusions on a 24 x 7 x 365 basis?
Answer: Yes
Provider edge monitoring operates 24x7x365; application security alerts email the district contact and help@breatheasy.net.

HFIH-01
Do you have a formal incident response plan?
Answer: Yes
Published incident response policy: severity classification, detect-contain-eradicate-recover-notify-review sequence, 72-hour notification, 15-business-day post-incident report.

HFIH-02
Do you either have an internal incident response team or retain an external team?
Answer: Yes
Internal response led by the security officer with provider support channels.

HFIH-03
Do you have the capability to respond to incidents on a 24 x 7 x 365 basis?
Answer: Yes
Security reports to help@breatheasy.net with 'SECURITY' in the subject are monitored continuously; automated lockout alerts are emailed immediately.

HFIH-04
Do you carry cyber-risk insurance to protect against unforeseen service outages, data that is lost or stolen, and security incidents?
Answer: Yes
Cyber-risk / technology errors and omissions coverage is carried through Hiscox with a $250,000 aggregate limit, policy period through February 24, 2027. A certificate of insurance, including a certificate naming the district, is issued on request. Breach cooperation and cost terms are stated in the district addendum and set in the signed agreement.

VULN-01
Are your systems and applications scanned with an authenticated user account for vulnerabilities (that are remediated) prior to new releases?*
Answer: Yes
Dependency and application security reviews are part of release preparation; known high-severity issues are resolved before affected changes deploy.

VULN-02
Will you provide results of application and system vulnerability scans to the institution?*
Answer: Yes
A summary of the most recent security review is available to districts on request.

VULN-03
Will you allow the institution to perform its own vulnerability testing and/or scanning of your systems and/or application, provided that testing is performed at a mutually agreed upon time and date?*
Answer: Yes
District testing can be scheduled at a mutually agreed time.

VULN-04
Have your systems and applications had a third-party security assessment completed in the last year?

Answer: No

No third-party security assessment in the last year; provider SOC 2 Type II reports cover the infrastructure layer.

VULN-05

Do you regularly scan for common web application security vulnerabilities (e.g., SQL injection, XSS, XSRF, etc.)?

Answer: Yes

Common web vulnerability classes (injection, XSS, CSRF) are addressed by framework defaults, parameterized database access, and release-preparation review.

VULN-06

Are your systems and applications regularly scanned externally for vulnerabilities?

Answer: No

External vulnerability scanning is covered at the infrastructure layer by the providers; the application layer is reviewed during release preparation.

IT Accessibility

ITAC-01

Solution Provider Accessibility Contact Name

Answer: Customer Support

ITAC-02

Solution Provider Accessibility Contact Title

Answer: Accessibility contact

ITAC-03

Solution Provider Accessibility Contact Email

Answer: help@breatheasy.net

ITAC-04

Solution Provider Accessibility Contact Phone Number

Answer: Not published; all support is handled by email at help@breatheasy.net

ITAC-05

Web Link to Accessibility Statement or VPAT

Answer: https://campus.breatheasy.net/compliance

ITAC-06

Has a VPAT or ACR been created or updated for the solution and version under consideration within the past 12 months?*

Answer: No

A formal VPAT/ACR has not been produced in the past 12 months; the accessibility standard and conformance process are published on the compliance page.

ITAC-07

Will your company agree to meet your stated accessibility standard or WCAG 2.1 AA as part of your contractual agreement for the solution?*

Answer: Yes

WCAG 2.1 AA is the stated contractual standard for the solution.

ITAC-08

Does the solution substantially conform to WCAG 2.1 AA?*

Answer: Yes

The application is built and reviewed against WCAG 2.1 AA: semantic structure, keyboard access, contrast targets, labeled controls, and screen-reader behavior on staff and student-facing surfaces.

ITAC-09

Do you have a documented and implemented process for reporting and tracking accessibility issues?*

Answer: Yes

Accessibility issues are reported to help@breatheasy.net, tracked to resolution, and verified on the affected pages.

ITAC-10

Do you have documentation to support the accessibility features of your solution?

Answer: Yes

The accessibility statement and commitments are published at campus.breatheasy.net/compliance.

ITAC-11

Has a third-party expert conducted an audit of the most recent version of your solution?

Answer: No

No third-party accessibility audit has been conducted; conformance is verified in-house against WCAG 2.1 AA criteria.

ITAC-12

Do you have a documented and implemented process for verifying accessibility conformance?

Answer: Yes

Accessibility checks are part of page-level review before release, including keyboard operation and screen-reader labeling.

ITAC-13

Have you adopted a technical or legal standard of conformance for the solution?

Answer: Yes

WCAG 2.1 AA.

ITAC-14

Can you provide a current, detailed accessibility roadmap with delivery timelines?

Answer: No

No separate accessibility roadmap document is published; conformance work is tracked as standard product work.

ITAC-15

Do you expect your staff to maintain a current skill set in IT accessibility?

Answer: Yes

Accessibility criteria are part of the standard development skill set and review checklist.

ITAC-16

Do you have documented processes and procedures for implementing accessibility into your development lifecycle?

Answer: Yes

Accessibility is part of the definition of done for new screens and is checked before release.

ITAC-17

Can all functions of the application or service be performed using only the keyboard?

Answer: Yes

All application functions are operable by keyboard.

ITAC-18

Does your product rely on activating a special "accessibility mode," a "lite version," or using an alternate interface (including “overlay” or AI-based alternates) for accessibility purposes?

Answer: No

No separate accessibility mode, overlay, or alternate interface is used.

Case-Specific

PCID-09

Describe the architecture employed by the system to verify and authorize credit card transactions.

Answer: Insert your answer here.

PCID-10
What payment processors/gateways does the system support?
Answer: Insert your answer here.

PCID-12
Include documentation describing the system's abilities to comply with the PCI DSS and any features or capabilities of the system that must be added or changed in order to operate in compliance with the standards.
Answer: Insert your answer here.

OPEM-08
Describe or provide a reference to any other safeguards used to monitor for malicious activity.
Answer: Insert your answer here.

OPEM-09
Describe how long your organization has conducted business in this area.
Answer: Insert your answer here.

AI

AIQU-01
Does your solution leverage machine learning (ML) or do you plan to do so in the next 12 months?
Answer: Yes
On-device face comparison models support the optional facial lookup capability, which is disabled by default and only appears after a district asks for it to be enabled. Frames are processed on the staff device and are not stored.

AIQU-02
Does your solution leverage a large language model (LLM) or do you plan to do so in the next 12 months?
Answer: Yes
Large language model access powers limited drafting suggestions, through a managed commercial gateway with no training on district data.

AIGN-01
Does your solution have an AI risk model when developing or implementing your solution's AI model?*
Answer: No
No formal AI risk model document; AI features are limited, optional, and district-controlled.

AIGN-02
Can your solution's AI features be disabled by tenant and/or user?*
Answer: Yes
AI features can be disabled per district on request.

AIGN-03
Have your staff completed responsible AI training?*
Answer: Yes

AIGN-04
Please describe the capabilities of your solution's AI features.
Answer: AI use is limited to drafting suggestions (for example, accommodation wording) reviewed by staff before saving, and on-device face comparison for the optional, district-authorized facial lookup.

AIGN-05
Does your solution support business rules to protect sensitive data from being ingested by the AI model?
Answer: Yes
AI features receive only the minimal context required for the specific drafting task; restricted records are not sent to AI services.

AIPL-01

Are your AI developer's policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks conspicuously posted, unambiguous, and implemented effectively?*

Answer: No

AI practices are documented in this questionnaire and the packet rather than a separate posted AI policy.

AIPL-02

Have you identified and measured AI risks?*

Answer: No

AI risk is handled through limitation of scope: optional features, minimal context, no training on district data, district-controlled enablement.

AIPL-03

In the event of an incident, can your solution's AI features be disabled in a timely manner?*

Answer: Yes

AI features can be disabled for a district promptly on request.

AIPL-04

If disabled because of an incident, can your solution's AI features be re-enabled in a timely manner?*

Answer: Yes

AIPL-05

Do you have documented technical and procedural processes to address potential negative impacts of AI as described by the AI Risk Management Framework (RMF)?

Answer: No

No separate NIST AI RMF process; the scope-limitation approach above is used.

AISC-01

If sensitive data is introduced to your solution's AI model, can the data be removed from the AI model by request?*

Answer: Yes

AI services do not retain district data for training, so there is nothing to remove from a model; source records are deleted per the retention schedule.

AISC-02

Is user input data used to influence your solution's AI model?*

Answer: No

AISC-03

Do you provide logging for your solution's AI feature(s) that includes user, date, and action taken?*

Answer: Yes

Each AI drafting run is written to the security event log with the acting user, email, timestamp, IP address, the specific AI tool used, the model, and the student record it was run against. District IT and district administrators review and export these events from the admin console.

AISC-04

Please describe how you validate user inputs.

Answer: All input is validated on the server, and privileged actions are re-checked server-side.

AISC-05

Do you plan for and mitigate supply-chain risk related to your AI features?

Answer: Yes

AI capability is sourced through a single managed commercial gateway under enterprise terms.

AIML-01

Do you separate ML training data from your ML solution data?*

Answer: Yes

The company does not train ML models on district data; face comparison uses pre-trained models running on the staff device.

AIML-02
Do you authenticate and verify your ML model's feedback?*
Answer: No
No model training is performed, so no training feedback loop exists.

AIML-03
Is your ML training data vetted, validated, and verified before training the solution's AI model?
Answer: N/A
The company does not train ML models.

AIML-04
Is your ML training data monitored and audited?
Answer: N/A
The company does not train ML models.

AIML-05
Have you limited access to your ML training data to only staff with an explicit business need?
Answer: N/A
The company does not train ML models.

AIML-06
Have you implemented adversarial training or other model defense mechanisms to protect your ML-related features?
Answer: No

AIML-07
Do you make your ML model transparent through documentation and log inputs and outputs?
Answer: Yes
AI behavior and limits are documented in this questionnaire and the district packet.

AIML-08
Do you watermark your ML training data?
Answer: N/A
No ML training data exists.

AILM-01
Do you limit your solution's LLM privileges by default?*
Answer: Yes
LLM access is limited to the specific drafting features; no tool or plugin execution.

AILM-02
Is your LLM training data vetted, validated, and verified before training the solution's AI model?*
Answer: N/A
The company does not tune or train LLMs.

AILM-03
Do any actions taken by your solution's LLM features or plugins require human intervention?*
Answer: Yes
AI output is a draft that staff must review and save; no automated actions are taken by the LLM.

AILM-04
Do you limit multiple LLM model plugins being called as part of a single input?*
Answer: Yes
No plugin chaining is used.

AILM-05
Do you limit your solution's LLM resource use per request, per step, and per action?

Answer: Yes

Requests are small, single-purpose drafting calls.

AILM-06

Do you leverage LLM model tuning or other model validation mechanisms?

Answer: No

Privacy

PRGN-01

Does your solution process FERPA-related data?

Answer: Yes

The company acts as a school official with legitimate educational interest under FERPA, 34 CFR 99.31(a)(1)(i)(B).

PRGN-02

Does your solution process GDPR-related or PIPL-related data?

Answer: No

The service operates in United States regions only for US districts.

PRGN-03

Does your solution process personal data regulated by state law(s) (e.g., CCPA)?

Answer: Yes

State student-privacy statutes apply; Nevada NRS 388.267-388.296 terms ship by default, and CA, TX, IL, and NY addenda are available.

PRGN-04

Does your solution process user-provided data that may contain regulated information?

Answer: Yes

All user-provided data is treated as potentially regulated and handled under the Schedule of Data.

PRGN-05

Web Link to Product/Service Privacy Notice

Answer: https://campus.breatheasy.net/privacy

PCOM-01

Have you had a personal data breach in the past three years that involved reporting to a governmental agency, notice to individuals (including voluntary notice), or notice to another organization or institution?*

Answer: No

PCOM-02

Use this area to share information about your privacy practices that will assist those who are assessing your company data privacy program.*

Answer: Data minimization is contractual: a published list of data categories we do not collect (SSNs, health records, lunch status, payment data, imported discipline history, and more). No advertising, no sale of data, no profiling. The Schedule of Data lists every stored element with purpose and retention.

PCOM-03

Have you had any violations of your internal privacy policies or violations of applicable privacy law in the past 36 months?

Answer: No

PCOM-04

Do you have a dedicated data privacy staff or office?

Answer: Yes

BreathEasy Administrative Services LLC is a two-member company. Both members perform operational duties. One member is designated security officer and incident commander; the other is designated privacy officer and backup incident commander, so

incident response and district contact do not depend on one person. Privacy contact is help@breatheasy.net.

PDOC-01

If you have completed a SOC 2 audit, does it include the Privacy Trust Service Principle?

Answer: N/A

BreathEasy Administrative Services LLC does not currently hold its own SOC 2 report. Underlying infrastructure (AWS, Cloudflare) operates under SOC 2 Type II and ISO 27001 certifications; provider reports are available on request. This completed questionnaire, the published security policy, and the named sub-processor list are provided for review.

PDOC-02

Do you conform with a specific industry-standard privacy framework (e.g., NIST Privacy Framework, GDPR, ISO 27701)?

Answer: No

Policies are written to FERPA and state student-privacy statute requirements; no formal privacy framework certification is held.

PDOC-03

Does your employee onboarding and offboarding policy include training of employees on information security and data privacy?

Answer: Yes

Confidentiality, data-handling, and FERPA training are part of onboarding; access is revoked the same day a role ends.

PTHP-01

Do you have contractual agreements with third parties that require them to maintain standards and to comply with all regulatory requirements?*

Answer: Yes

Sub-processor terms are at least as restrictive as the district agreement.

PTHP-02

Do you perform privacy impact assessments of third parties that collect, process, or have access to personal data to ensure they meet industry and regulatory standards and to mitigate harmful, unethical, or discriminatory impacts on data subjects?

Answer: Yes

Sub-processors are reviewed for security and privacy posture before use; districts are notified before changes affecting student data.

PCHG-01

Does your change management process include privacy review and approval?

Answer: Yes

Material changes affecting student data are communicated to district contacts before taking effect.

PCHG-02

Do you have policy and procedure, currently implemented, guiding how privacy risks are mitigated until they can be resolved?

Answer: Yes

Privacy-affecting changes are held until the policy text and district notice are updated.

PDAT-01

Do you collect, process, or store demographic information?*

Answer: No

No demographic information is collected beyond the roster fields in the Schedule of Data (name, grade, homeroom/section, identifiers).

PDAT-02

Do you capture or create genetic, biometric, or behaviometric information (e.g., facial recognition or fingerprints)?*

Answer: Yes

Only when a district authorizes and enables the optional facial lookup capability, which is disabled by default at the district level: reference images and mathematical face templates. Live camera frames are processed on the staff device and are not stored. No

fingerprints or voiceprints are collected.

PDAT-03
Do you combine institutional data (including "de-identified," "anonymized," or otherwise masked data) with personal data from any other sources?*

Answer: No
District data is never combined with data from other sources.

PDAT-04
Is institutional data coming into or going out of the United States at any point during collection, processing, storage, or archiving?

Answer: No
All collection, processing, storage, and archiving occur in United States regions.

PDAT-05
Do you capture device information (e.g., IP address, MAC address)?

Answer: Yes
IP address and user agent are recorded in security event logs for sign-in and administrative events; retention 18 months. No MAC addresses.

PDAT-06
Does any part of this service/project involve a web/app tracking component (e.g., use of web-tracking pixels, cookies)?

Answer: No
No tracking pixels, cookies, or third-party analytics. The public website uses cookie-free, anonymous page-view measurement (path, timestamp, referrer domain, device type, daily-rotating hash) that cannot be tied to a person.

PDAT-07
Does your staff (or a third party) have access to institutional data (e.g., financial, PHI, or other sensitive information) through any means?

Answer: Yes
Named company personnel, for support and maintenance only, with access logged.

PDAT-08
Will you handle personal data in a manner compliant with all relevant laws, regulations, and applicable institution policies?

Answer: Yes

PRPO-01
Do you have a documented privacy management process?

Answer: Yes
Documented privacy policy, data classification, retention schedule, and Schedule of Data.

PRPO-02
Are privacy principles designed into the product lifecycle (i.e., privacy-by-design)?

Answer: Yes
Data minimization and least-privilege defaults are built into the product.

PRPO-03
Will you comply with applicable breach notification laws?

Answer: Yes
72-hour maximum notification after confirmation of a breach involving district data.

PRPO-04
Will you comply with the institution's policies regarding user privacy and data protection?

Answer: Yes

PRPO-05

Is your company subject to the laws and regulations of the institution's geographic region?

Answer: Yes

PRPO-06

Do you have a privacy awareness/training program?*

Answer: Yes

Annual security awareness and FERPA training.

PRPO-07

Is privacy awareness training mandatory for all employees?

Answer: Yes

PRPO-08

Is AI privacy and ethics awareness/training required for all employees who work with AI?

Answer: Yes

Staff working with AI features are trained on the rule that district data is never used to train models.

PRPO-09

Do you have any decision-making processes that are completely automated (i.e., there is no human involvement)?

Answer: No

No fully automated decision-making; all consequential actions are taken by district staff.

PRPO-10

Do you have a documented process for managing automated processing, including validations, monitoring, and data subject requests?

Answer: N/A

No completely automated decision-making processes.

PRPO-11

Do you have a documented policy for sharing information with law enforcement?

Answer: Yes

Information is disclosed to law enforcement only when legally required, and the district is informed first unless legally prohibited.

PRPO-12

Do you share any institutional data with law enforcement without a valid warrant or subpoena?*

Answer: No

PRPO-13

Does your incident response team include a privacy analyst/officer?

Answer: Yes

The security officer also holds privacy responsibilities in incident response.

INTL-01

Will data be collected from or processed in or stored in the European Economic Area (EEA)?

Answer: No

INTL-02

Do you have a data protection officer (DPO)?

Answer: No

A privacy officer role is designated to one of the two company members; a formal DPO under GDPR Article 37 is not appointed.

INTL-03

Will you sign appropriate GDPR Standard Contractual Clauses (SCCs) with the institution?

Answer: N/A

No EEA processing.

INTL-04
Will data be collected from or processed in or stored in China?

Answer: No

INTL-05
Do you comply with PIPL security, privacy, and data localization requirements?

Answer: N/A

No processing in China.

DRPV-01
Have you performed a Data Privacy Impact Assessment for the solution/project?

Answer: No

A formal DPIA has not been conducted; the Schedule of Data, data minimization list, and data flow documentation serve the same review purpose and are published.

DRPV-02
Do you provide an end-user privacy notice about privacy policies and procedures that identify the purpose(s) for which personal information is collected, used, retained, and disclosed?

Answer: Yes

The privacy notice is public and linked from every page.

DRPV-03
Do you describe the choices available to the individual and obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information?

Answer: Yes

The district agreement defines the authorized scope; for students under 13 the school provides COPPA consent as the parent's agent.

DRPV-04
Do you collect personal information only for the purpose(s) identified in the agreement with an institution or, if there is none, the purpose(s) identified in the privacy notice?

Answer: Yes

Data is used only to deliver the contracted service.

DRPV-05
Do you have a documented list of personal data your service maintains?

Answer: Yes

The published Schedule of Data lists every data element, source, purpose, and retention.

DRPV-06
Do you retain personal information for only as long as necessary to fulfill the stated purpose(s) or as required by law or regulation and thereafter appropriately dispose of such information?

Answer: Yes

Published retention periods; deletion within 30 days on request or contract end, backups aging out at 35 days.

DRPV-07
Do you provide individuals with access to their personal information for review and update (i.e., data subject rights)?

Answer: Yes

Requests are handled by the district as record holder; the company forwards and supports any request it receives.

DRPV-08
Do you disclose personal information to third parties only for the purpose(s) identified in the privacy notice or with the implicit or explicit consent of the individual?

Answer: Yes

Disclosure only as the district instructs or law requires, with prior notice to the district unless prohibited.

DRPV-09
Do you protect personal information against unauthorized access (both physical and logical)?
Answer: Yes
Encryption, database-enforced tenancy, least privilege, and account lockout.

DRPV-10
Do you maintain accurate, complete, and relevant personal information for the purposes identified in the privacy notice?
Answer: Yes
District staff control and correct records; audit-sensitive records are append-only with timestamped amendments.

DRPV-11
Do you have procedures to address privacy-related noncompliance complaints and disputes?
Answer: Yes
Privacy complaints go to help@breatheasy.net and are handled with the district.

DRPV-12
Do you "anonymize," "de-identify," or otherwise mask personal data?
Answer: No
No anonymization or de-identification pipeline is operated; district data is not used outside the district's service.

DRPV-13
Do you or your subprocessors use or disclose "anonymized," "de-identified," or otherwise masked data for any purpose other than those identified in the agreement with an institution (e.g., sharing with ad networks or data brokers, marketing, creation of profiles, analytics unrelated to services provided to institution)?
Answer: No

DRPV-14
Do you certify stop-processing requests, including any data that is processed by a third party on your behalf?
Answer: Yes
Stop-processing and deletion requests are certified in writing, including sub-processor copies aging out on the backup cycle.

DRPV-15
Do you have a process to review code for ethical considerations?
Answer: No
No formal ethics code-review process; automated decision-making is not used.

DPAI-01
Does your service use AI for the processing of institutional data?
Answer: Yes
Limited AI-assisted drafting (for example, suggested accommodation text). AI output is a suggestion that staff review before saving.

DPAI-02
Is any institutional data retained in AI processing?*
Answer: No
AI requests are processed per-request; institutional data is not retained by the AI service for training.

DPAI-03
Do you have agreements in place with third parties or subprocessors regarding the protection of customer data and use of AI?*
Answer: Yes
AI processing occurs under provider terms that prohibit use of customer data for model training.

DPAI-04
Will institutional data be processed through a third party or subprocessor that also uses AI?
Answer: Yes

Only for the limited AI drafting features, through a managed commercial AI gateway; no training on district data.

DPAI-05
Is AI processing limited to fully licensed commercial enterprise AI services?
Answer: Yes
Only licensed commercial AI services are used.

DPAI-06
Will institutional data be used or processed by any shared AI services?
Answer: No
District data is not processed by shared AI training pipelines.

DPAI-07
Do you have safeguards in place to protect institutional data and data privacy from unintended AI queries or processing?
Answer: Yes
AI features are limited to specific drafting tasks with minimal context, and can be disabled per district on request.

DPAI-08
Do you provide choice to the user to opt out of AI use?
Answer: Yes
Districts may have AI features disabled on request.