District — `{{school_name}}`

SIGNATURE	DATE
PRINTED NAME	TITLE

EXHIBIT A — ASKELIRA DATA SECURITY AND PRIVACY PLAN

THIRD-PARTY CONTRACTOR PLAN UNDER 8 NYCRR § 121.6 · VERSION 3.0 · AUGUST 2026

Status of this Exhibit

This Exhibit A is **the** Data Security and Privacy Plan required by 8 NYCRR § 121.6. It is complete in itself: there is no separate standalone Plan, no summary version, and nothing to read alongside it. The educational agency accepts this Plan by executing the Addendum, and the executed Addendum controls. Section 8 states the implemented controls as reviewed in the production deployment and code on **July 24, 2026**. This is a statement of control-level alignment, **not a certification**.

1. Contractor, role, and scope

stoplosses.ai LLC (the "Contractor"), a Wyoming limited liability company with its principal address at 3660 Oxford Ave, Bronx, NY 10463, provides automated charter-school enrollment- and attendance-outreach services. For each contracting school (the "Educational Agency" or "Agency"), the Agency is the data Controller and the Contractor is a third-party contractor and Processor, and a FERPA "school official" where the conditions in DPA § 2.2 are met. This Plan is submitted for the Agency's acceptance and attached to the executed § 2-d Addendum. It demonstrates control-level alignment with the NIST Cybersecurity Framework, the standard adopted under 8 NYCRR § 121.5, and is designed to comply with the Agency's own data security and privacy policy.

2. § 121.6(a)(1) — How the Contractor implements the data security and privacy requirements over the life of the contract

The Contractor implements the state, federal, and local data security and privacy requirements of this contract through the controls in Sections 3 through 9 of this Plan, which are contractual obligations under the executed Data Processing Agreement and § 2-d Addendum, not aspirations. Under § 2-d Addendum § 2(b) and 8 NYCRR § 121.9(a)(2), the Contractor complies with the Agency's own data security and privacy policy as updated from time to time, on written notice of any update. Controls are reviewed against the production deployment at least annually and on any material change to data-handling practices, and the Agency receives an updated Plan on written request and in advance of any material change. Controls are sized to the Contractor's current scale and reviewed as school volume grows; open items — for example SOC 2 timing, and the subprocessor limitations

disclosed in Section 5 — are disclosed rather than papered over. On **July 27, 2026** the Contractor migrated all model inference from a developer API to an enterprise cloud provider serving a US Processing Endpoint, which is what permits the in-region processing statement in Section 5.

3. § 121.6(a)(2) — Administrative, operational, and technical safeguards in place

3.1 Data elements received

Only minimized enrollment and attendance data, enumerated exhaustively in DPA § 3.1(a): guardian name, phone, email, preferred language; student first name; student full name (attendance alerts only); seat/application status; the school system's student and application record identifiers; enrollment grade level (not an academic or report-card grade) and campus; waitlist position; registration-paperwork checklist status (which documents are in or missing, never their contents); an IEP yes/no flag and an IEP-file-attached yes/no flag (no classification, services, or document contents); staff enrollment notes (Social-Security-number-shaped text redacted before storage); attendance status (present/absent, where enabled); enrollment year; guardian question text submitted to the family Q&A assistant; inbound message metadata; and the outcome plus a brief summary of each automated call or message. **No audio recordings or transcripts are created** — voice is a deterministic keypad IVR. Agency staff and account data is enumerated separately in DPA § 3.1(b). The categories in DPA § 3.2 are prohibited outright.

3.2 Technical safeguards

- **Encryption in transit.** TLS 1.2 or higher on every connection carrying Protected Data; TLS 1.3 at the public edge. The public service redirects HTTP to HTTPS and publishes HSTS. Outbound connections to each subprocessor listed in Section 6 use HTTPS or secure libSQL transport and support TLS 1.2+. The Contractor does not claim that every subprocessor connection negotiates TLS 1.3.
- **Encryption at rest.** Provider-managed storage and volume-level encryption on U.S.-based managed infrastructure (Turso Cloud). Database credentials are obtained from Vercel Sensitive environment variables. **The Contractor has not configured Turso BYOK page-level encryption and does not represent that its database pages use AES-256-GCM or AEGIS-256.**
- **Credential envelope.** School-system credentials submitted through the dashboard (for example SchoolMint logins) are sealed before database storage with AES-256-GCM under a random per-envelope key, wrapped using RSA-OAEP with SHA-256. Cloud systems store ciphertext; wrapping-key material is held as a protected runtime secret available to the authorized application and operations runtime, **not** as cleartext in the database. **The envelope protects database contents and backups; it is not represented as opaque to an authorized application runtime.**

- **Authentication. Multi-factor authentication is enforced on every account of the Contractor's own application, including every administrator account, with no exemption.** A sign-in requires two independent factors, in sequence: a password belonging to that one person, verified first and stored only as a salted cryptographic digest (scrypt, per-user random salt) — never as the password itself, never in a recoverable form, never logged and never transmitted by email; and then a single-use sign-in link sent to that person's verified email address, expiring in five minutes. **A correct password alone never establishes a session; the emailed link is always required**, so neither a compromised mailbox nor a compromised password is sufficient by itself. Each named user, including each colleague invited to a school's dashboard, sets their own password before the dashboard renders anything, so no two people share a factor. Password attempts are rate-limited per account and per source, and every authentication outcome is written to the security-event log described in Section 3.3. Multi-factor authentication is additionally maintained on the underlying infrastructure-provider consoles under the Contractor's administrative attestation.
- **Access control.** Access to Protected Data is restricted to personnel with a documented, role-based need. Vercel environment variables are encrypted at rest and security credentials are maintained as non-readable Sensitive variables restricted to authorized project personnel.
- **Webhook and job authorization.** All deployed scheduled routes fail closed unless presented with an authorized cron or API secret. Twilio, Stripe, and eSignatures webhooks use fail-closed signature validation. Inbound mail processing uses authenticated provider polling and excludes messages lacking the receiving provider's authentication verdict. DNS-resolution and private-address protections apply to user-supplied public-preview website fetches.
- **Logging.** Security-relevant events — authentication attempts and failures, credential-envelope retrievals, material database row-count changes, outbound-send anomalies — are logged with actor, timestamp, and coarsened source IP, retained a minimum of 90 days, and swept by automated scans every 30 to 60 minutes. **Security-event records are conventional database audit records and are not represented as cryptographically tamper-evident.**
- **Secret handling.** Third-party integration keys are stored in access-controlled secret storage — encrypted platform environment variables, and a full-disk-encrypted operations workstation locally — never committed to source control and never logged.

3.3 Administrative and operational safeguards

- Written confidentiality obligations and NYS Education Law § 2-d policy acknowledgements, executed and re-certified annually by every person with access to Protected Data.
- Access privileges reviewed, and revoked promptly on termination of engagement.
- A written incident-response plan, provided to the Agency on request before go-live, and regular security reviews.
- A formal criminal background check on every person with access to Protected Data before access is granted, renewed at least annually. Such checks have been performed on all current personnel with access.
- Data minimization enforced in code as well as contract: the categories prohibited by DPA § 3.2 are not collected, and Social-Security-number-shaped text in staff notes is redacted before storage.

3.4 Physical safeguards

The Contractor operates no data center. All Protected Data resides on systems maintained by the subprocessors in Section 6, on United States regional settings, subject to the provider limitations disclosed in Section 5. Contractor workstations with any access to Protected Data use full-disk encryption and screen-lock controls.

4. § 121.6(a)(3) — Compliance with 8 NYCRR § 121.3(c)

The supplemental information required by § 121.3(c) must be developed by the Agency. The Contractor supplies complete vendor-side content for all six required items as **Exhibit B** to this Addendum, and will supply any further information the Agency requires to complete and publish its supplement under § 121.3(d):

§ 121.3(C) ITEMS AND WHERE THE VENDOR CONTENT APPEARS

§ 121.3(c) item	Vendor content
(1) Exclusive purposes for which the data will be used	Exhibit B (1); Section 5 of this Plan
(2) How subcontractors will abide by data-protection requirements	Exhibit B (2); Sections 6 and 7 of this Plan
(3) Contract duration, expiration date, and what happens to the data on expiration	Exhibit B (3); Section 9 of this Plan. The expiration date itself comes from the Agency's executed Order Form and is completed by the Agency
(4) If and how a parent, student, teacher, or principal may challenge data accuracy	Exhibit B (4); § 2-d Addendum § 8
(5) Where the data will be stored and the security protections applied	Exhibit B (5); Sections 3 and 6 of this Plan
(6) How the data is protected using encryption in motion and at rest	Exhibit B (6); Section 3.2 of this Plan

5. Exclusive purposes

Protected Data is used only to run the Agency's enrollment and attendance outreach: family SMS and email sequences; weekday enrollment voice calls via a deterministic Twilio keypad IVR (press 1 to accept, press 2 to decline, press 9 for the main office, press 7 to report a wrong number, press 8 to stop the calls), each call stating the Agency's main office telephone number as required by 47 CFR § 64.1200(b)(2); same-day attendance notices — comprising the absence notice and, **where the Agency switches it on, a late-arrival (tardy) notice sent as one bilingual text message only, no call and no email, no more than once per student per school day**, which is off unless the Agency enables it and which the Contractor will not enable for an Agency whose captured consent language does not disclose it — which name the student in full in text and email and by first name only in the spoken announcement, and offer a press-6 keypad option that stops the calls while the text and email notices continue, reversible by texting CALLS, alongside the same press-7, press-8 and press-9 keys the enrollment calls carry; IEP-director notification; the daily operations digest; roster and tracker auto-fill; the family Q&A assistant; the automated send-or-hold review of Staff Enrollment Notes before an outbound message is released; and, where the Agency's uploads carry present-day records, attendance measures computed for the Agency's own staff inside the Agency's own dashboard — each student's attendance rate against the days that student was enrolled, the chronic-absence determination that follows under the New York definition, and an early warning where a student is projected to cross that line, each shown with the numerator, denominator and threshold that produced it. Those measures produce no risk score and no prediction beyond that stated arithmetic, are never disclosed outside the Agency's own dashboard, and drive no automated contact of any kind: every action a measure suggests is a recommendation for Agency staff to take or not take. Where the

Agency's uploads carry absences only, the Contractor reports absence counts and declines to state a rate or a chronic determination rather than assume a denominator it was not given. **No sale, no marketing, and no use of Agency data to train or improve any AI or machine-learning model.**

Residency, stated plainly. The Contractor's own systems are configured to United States regions: the database (Turso) in U.S. data centers, application hosting and the serverless runtime on Vercel, message delivery through Twilio and Amazon SES, all on U.S. settings, with no Contractor-operated store or backup outside the United States. Authorized Contractor personnel may administer the Platform from outside the United States over an encrypted connection to those United States-hosted systems, under enforced multi-factor authentication. Such access creates no store, copy, or backup of Protected Data outside the United States, and all scheduled processing of Protected Data runs on United States-hosted infrastructure. **The Contractor does not, however, warrant that no Protected Data ever leaves the United States**, because its providers do not give it that warranty: model inference runs on the AI model provider or providers listed in DPA § 5.3(a) (published at schools.askelira.com/legal/subprocessors), each through a US Processing Endpoint, where the provider commits that data at rest and model processing stay in the selected region, subject only to the abuse-monitoring retention stated for that provider in the schedule (for Google Cloud Vertex AI, up to 90 days in that same region; for Amazon Web Services (Amazon Bedrock), none — zero data retention is that service's default and nothing is stored); Vercel states that it may process data globally and replicates some backups globally; Twilio states that selecting a region does not guarantee that every datum remains in that region; and **Meta, which operates the WhatsApp network, gives no United States processing commitment at all** — a channel that exists only because a guardian chose to write from WhatsApp, where they are already Meta's own user under terms Meta presents to them directly, and where AskElira stores no part of the exchange — it carries that traffic over its own global infrastructure, and unlike the other two this exposure is the message *content* a guardian writes and the answer sent back, not only metadata or a replicated backup. **The Contractor verifies the configured region of the AI endpoint at least quarterly, and on any change of model provider or cloud project, records the result, and provides that record to the Agency on written request.**
AI inference is in-region. Content is sent to an AI model provider listed in DPA § 5.3(a) through a US Processing Endpoint (the region is recorded in the Order Form; `us-central1` unless stated otherwise). For Google Cloud Vertex AI, the provider currently listed there, Google commits that customer data stored at rest remains in the selected region and that ML processing occurs within that region, and Google does not use the content to train or improve its models. The residual exception is Google's own abuse monitoring, which may retain prompts and responses for a limited period; an exemption process exists and The Contractor has not yet applied for it. The AI functions in DPA § 3.5 are core Platform functionality and are **not** offered on an opt-out basis.

6. § 121.6(a)(5) — Subcontractors, and how those relationships are managed

The Contractor uses a limited, disclosed set of subprocessors. Each is bound by written data-protection terms covering confidentiality, security, breach notification, and deletion on the Contractor's instruction — with the single exception of Meta Platforms, named below, which accepts no deletion instruction for WhatsApp message content and whose channel is therefore off unless the Agency switches it on. The Contractor remains liable to the Agency for their acts and omissions. Where a provider publishes standard terms the Contractor cannot negotiate, AskElira imposes on each subprocessor, by written agreement, data-protection obligations no less protective than those AskElira owes the Agency, as **8 NYCRR § 121.9(b)** requires. Where a provider publishes standard terms AskElira cannot negotiate, AskElira selects only providers whose published terms meet that standard, and configures each service to United States regions where the provider offers that control. **One**

exception, named rather than disclaimed: Meta Platforms. Meta operates the WhatsApp network on its own published terms, gives no United States processing commitment, and does not accept deletion instructions from AskElira for message content crossing its network. That is why the WhatsApp channel is **off unless the Agency switches it on**, and why leaving it off costs the Agency nothing else in the Services. Rows marked AI model provider are the providers referred to in DPA § 3.5; where more than one is listed, each is engaged only for the functions stated in its row. The Agency receives not less than **30 days'** advance written notice before any addition or replacement of a subcontractor with access to Protected Data, and an opportunity to object; if the objection cannot be accommodated, the Agency may terminate without penalty. **This schedule reproduces DPA § 5.3(a), which is the single authoritative list and controls on any difference.** DPA § 5.3(a) is published at **schools.askelira.com/legal/subprocessors**; the table below is that schedule as of Version 3.0 · August 2026.

SUBPROCESSORS WITH ACCESS TO PROTECTED DATA

Subprocessor	Role	Protected Data accessed	Location
Twilio, Inc.	SMS (A2P 10DLC) + keypad-IVR voice + plain-TTS attendance calls	Guardian phone; student first name (spoken in enrollment *and* attendance call scripts); student full name (attendance text and email only); seat/attendance status; call outcome	US region; **provider does not guarantee every datum stays in region**
Meta Platforms, Inc. *WhatsApp Business Platform*	Carries family Q&A assistant messages over WhatsApp, where the Agency enables that channel; reached through Twilio's WhatsApp Business API, with Twilio the provider of record and Meta operating the network and receiving the message content	Guardian WhatsApp number and display name; guardian question text; assistant answer text. Section 3.1(a) enrollment and attendance records are **not** sent over this channel	**Global; provider gives no US processing commitment** — see Section 5 of this Plan
Google Cloud — Vertex AI	**AI model provider (DPA § 3.5)**: family Q&A assistant, staff support assistant, School Operational Document reading. Content is not used to train or improve Google's models	Guardian question text; School Operational Documents the School uploads (flyers, calendars)	**US regional endpoint**; at rest and ML processing in-region; abuse-monitoring retention up to 90 days, held in the selected region, not used for training

Subprocessor	Role	Protected Data accessed	Location
Amazon Web Services — Amazon Bedrock	**AI model provider (DPA § 3.5)**: staff-note send/hold review. The model served was developed by DeepSeek and is operated entirely by AWS; the developer receives no content, and content is not used to train or improve any model	Staff Enrollment Notes (review only)	**US regional endpoint** (us-east-1, us-east-2 or us-west-2); cross-Region routing unsupported for this model. Zero data retention, zero operator access — nothing stored
Google LLC — Sheets API	Enrollment tracker autofill	Enrollment data per DPA § 3.1(a)	US
Turso (ChiselStrike)	Primary database hosting, provider-managed volume-level encryption at rest	All persisted § 3.1 data	US
Vercel, Inc.	Application hosting **+ the serverless runtime that processes** Protected Data	All § 3.1 data in-runtime	US regions; **global processing and backup replication reserved by provider**
AgentMail (Amazon SES)	Outbound and inbound email, and receiving-provider authentication (SPF/DKIM/DMARC) of inbound guardian mail	Guardian email; student first name; full name (attendance emails only)	US
Resend, Inc.	**Standby** outbound email delivery, used only where the primary provider will not accept a message for transport. A rejection belonging to the recipient — suppression or block list — is never retried here. Inbound mail and its SPF/DKIM/DMARC authentication remain with AgentMail	Guardian email; student first name; full name (attendance emails only)	US
SchoolMint	Agency-authorized SIS integration	Guardian phone/email; first name; grade; seat status; campus; enrollment year; SIS identifiers	US

Not subprocessors of Protected Data. Anthropic PBC is used only as internal software-development tooling and never receives Protected Data. The former conversational-voice path (**VAPI**, with **OpenAI** as its model provider) was retired on July 24, 2026 and processes no Agency data. A provider's appearance in the schedule above is independent of that retired path. Spoken audio is generated by Twilio-native text-to-speech;

no third-party text-to-speech provider is used. **Stripe, Inc.** and **eSignatures.com** process Agency staff and billing data only, as disclosed in DPA § 5.3(b) and published at schools.askelira.com/legal/subprocessors, and receive no student or guardian data.

7. § 121.6(a)(4) — Training

Every officer, employee, and assignee of the Contractor with access to Protected Data receives training on the federal and state laws governing the confidentiality of that data — FERPA, NY Education Law § 2-d and 8 NYCRR Part 121, COPPA, PPRA, and IDEA as applicable — **before** receiving access, and at least annually thereafter. Completion is recorded and re-certified annually alongside the confidentiality and § 2-d policy acknowledgements in Section 3.3, and **the completion record is provided to the Agency on written request**, since this is the § 121.6(a)(4) commitment the Agency accepts by signing. Access to Protected Data is presently restricted to founding leadership — the Chief Executive Officer and the Chief Operating Officer — who hold direct NYS school-operations backgrounds. Where the NYSED Chief Privacy Officer orders additional training under 8 NYCRR § 121.11(e)(4), the Contractor provides it at its own expense and certifies completion.

8. § 121.6(a)(6) — Managing data security and privacy incidents

8.1 Detection

An automated breach-detection agent runs on an hourly schedule, as a cloud-scheduled job on the Contractor's production hosting platform, monitoring authentication anomalies, material database row-count changes, outbound-send spikes, and public breach information. Credential-envelope retrievals are recorded for investigation. Incident records create a 48-hour response deadline; notices to a live school require human acknowledgement and are deduplicated per incident and school. **The Chief Executive Officer is the on-call owner of that deadline and the Chief Operating Officer is the alternate.** If an incident notice to a live school is not acknowledged within four hours of being raised, the system re-alerts both officers by a second channel and continues at hourly intervals until acknowledged; an unacknowledged notice never suppresses or delays the 48-hour notice to the Agency, which is sent on the deadline regardless of whether the internal acknowledgement has occurred.

8.2 Notification

On discovering or reasonably suspecting a breach or unauthorized release, the Contractor notifies the Agency's designated Data Protection Officer by email in the most expedient way possible and without unreasonable delay, and **in no case more than 48 hours after discovery** — well inside the seven-calendar-day maximum for contractor-to-agency notice under 8 NYCRR § 121.10(a). The notice is plain and clear and includes, to the extent available, a description of the incident, the dates of the incident and of discovery, the types of Protected Data affected, an estimate of the number of records affected, the investigation or plan to investigate, and contact information for representatives who can assist parents or eligible students. A written incident report follows within five business days. The Contractor cooperates with the Agency and law enforcement, preserves evidence, does not contact the NYSED Chief Privacy Officer directly unless the Agency requests it or law requires it, and reimburses the Agency for the full reasonable and documented cost of notifications required under § 2-d where the incident is attributable to the Contractor's acts or omissions. **That reimbursement obligation is not subject to any cap in MSA § 11 or DPA § 12.3**, which expressly exclude it.

8.3 Security implementation review — July 24, 2026

The controls described in Sections 3, 6, and 8.1 were reviewed against the production deployment and source code on July 24, 2026, and the authentication control in Section 3.2 was re-reviewed against the deployed implementation and its automated test suite on August 1, 2026, when multi-factor authentication was enforced on all application accounts. They are stated as they actually exist, including the four explicit non-representations (no BYOK page-level database encryption; no claim that every subprocessor connection negotiates TLS 1.3; the credential envelope is not opaque to an authorized runtime; security-event records are not cryptographically tamper-evident). **The non-representation that multi-factor authentication was maintained only on provider consoles, and not enforced on the Contractor's own administrator accounts, was withdrawn on August 1, 2026 because the control it disclaimed is now implemented and enforced** — see Section 3.2. Implemented controls demonstrate control-level alignment — not certification — with NIST CSF v1.1 subcategories including ID.AM-3/4/5, ID.GV-3, ID.SC-2/3, PR.AC-1/4/7, PR.DS-1/2/5, PR.IP-6, PR.PT-1/3/4, DE.AE-2/3/5, DE.CM-7, DE.DP-4, RS.RP-1, RS.CO-1/2/3, RS.AN-1/2/4, and the corresponding CSF v2.0 outcomes.

9. § 121.6(a)(7) — Return, transition, deletion, and destruction

Retention and deletion follow the record-class matrix in DPA § 9, which governs. In summary: family-operational Protected Data is deleted after **90 days of inactivity** while the subscription is active; no audio or transcripts exist to delete. Within **30 days** of expiration without renewal or of termination, the Contractor ceases processing, provides a CSV export within 10 business days, and permanently deletes all remaining Protected Data from active production systems; subcontractors are instructed to delete the Protected Data they hold within **90 days**; backup and disaster-recovery copies are permanently deleted within **90 days**. At the Agency's option and direction, the Contractor instead transitions Protected Data to an Agency-designated successor contractor bound by data-protection agreements no less protective than this Addendum. **Redaction is not an acceptable means of destruction; destruction must render Protected Data permanently unreadable and unrecoverable.** Written certification from an authorized officer is provided on request. Consent, opt-out, and STOP or wrong-number suppression records are retained for the minimal period required to evidence TCPA and do-not-contact compliance under 47 CFR § 64.1200, and credential, send-ledger, and provider-held records follow the separate periods in the DPA § 9 matrix.

10. Compliance and incorporated documents

This Plan is designed to comply with the Agency's data security and privacy policy, NY Education Law § 2-d, 8 NYCRR Part 121, and FERPA. The Agency's adopted Parents' Bill of Rights is attached to this Addendum as Annex 1, and the vendor content for the Agency's § 121.3(c) supplement is Exhibit B.

stoplosses.ai LLC · Data Security & Privacy Plan v2.7 (8 NYCRR § 121.6) · Exhibit A to the NY Education Law § 2-d Addendum · Security implementation reviewed July 24, 2026.