NEW YORK EDUCATION LAW § 2-d ADDENDUM

VERSION 3.0 · AUGUST 2026 · STOPLOSSES.AI LLC · SCHOOLS.ASKELIRA.COM/LEGAL

Including **Exhibit A** (Data Security & Privacy Plan, 8 NYCRR § 121.6) and **Exhibit B** (vendor content for the educational agency's supplement to its Parents' Bill of Rights, 8 NYCRR § 121.3(c)).

PARTIES TO THIS ADDENDUM

District/School	`{{school_name}}` (the "District" or "School")
Vendor	stoplosses.ai LLC ("Vendor"), a Wyoming limited liability company
Effective Date	_____
Related Agreements	Incorporated by reference into, and **co-terminous with**, the AskElira for Schools Master SaaS & Services Agreement and Data Processing Agreement (collectively, the "Agreement")

This NY Education Law § 2-d Addendum ("Addendum") is entered into by `{{school_name}}` (the "District" or "School") and stoplosses.ai LLC ("Vendor"), effective as of the Effective Date. The parties agree to be bound by the Master SaaS & Services Agreement and Data Processing Agreement (collectively, the "Agreement"). This Addendum supplements and is incorporated by reference into the Agreement to ensure conformance with NY Education Law § 2-d and Part 121 of the Commissioner's Regulations ("NY 2-d"). **In the event of any direct conflict between this Addendum and the Agreement, this Addendum controls.** Except as expressly stated in § 6(c) of this Addendum, and except where prohibited by applicable law, any limitations on liability in the Agreement apply to this Addendum. **The obligation in § 6(c) to pay or promptly reimburse the District for the full cost of notifications required under 8 NYCRR § 121.10(f) is not subject to any cap, limitation, or exclusion in this Addendum, the Agreement, or the DPA, and no provision of any of them shall be read to qualify it.** The Agreement and this Addendum are collectively the "Full Agreement."

1. DEFINITIONS

As used herein, **"Protected Data"** means Student Data (as defined in NY 2-d) and/or Teacher or Principal Data (as defined in NY 2-d), including but not limited to: guardian name, phone number, email address, and preferred language; student first name; student full name (first and last, used solely for daily attendance text and email alerts — attendance voice announcements use the first name only); grade level (enrollment grade, not an academic/report-card grade); seat/application status (offered/accepted/declined/waitlisted); the school system's student and application record identifiers; waitlist position; attendance category for a school day (one of eight values — present, tardy, half day, excused absence, unexcused absence, out-of-school suspension, not enrolled, no session — normalized from the School's own status text at upload, with the School's free text and any stated reason for an absence discarded rather than stored; used for same-day attendance notifications and for the attendance measures shown to School staff in the School's own dashboard); IEP boolean flag (yes/no) and IEP-file-attached flag (yes/no); registration-paperwork checklist status; enrollment year; campus identifier; Staff Enrollment Notes (Social-Security-number-shaped text redacted before storage); **call/message outcome records** (disposition plus a brief operational summary — **no audio recording or transcript is created or retained**); **guardian question text** submitted to the family question-and-answer assistant through the

School's website chat widget, by inbound text message, or by inbound WhatsApp message; **inbound guardian email, SMS, and WhatsApp metadata** (provider message identifier, sender address or the last four digits of the sending number, and the classified outcome); and the **consent and revocation record** described in DPA § 3.1(a), each as further described in the AskElira Data Processing Agreement § 3.1. All other capitalized terms have the meanings given in NY 2-d.

2. VENDOR'S OBLIGATIONS AND CONFIDENTIALITY

(a) Vendor acknowledges that Protected Data received under the Full Agreement originates from the District and, as between the parties, belongs to and is under the control of the District. Vendor has no independent rights in Protected Data.

(b) Vendor will maintain the confidentiality of Protected Data in accordance with federal and state law (including NY 2-d, FERPA, COPPA, PPRA, and IDEA to the extent applicable) and the District's policy on data security and privacy. As required by 8 NYCRR § 121.9(a)(2), Vendor agrees to comply with the District's data security and privacy policy, as updated from time to time, upon receipt of written notice of any such update.

(c) Vendor will not sell Personally Identifiable Information nor use or disclose it for any Marketing or Commercial Purpose, nor facilitate or permit another party to do so.

(d) Vendor will limit internal access to Education Records to individuals with a legitimate educational interest within the meaning of NY 2-d and FERPA, and will limit access to PII to only those employees, third-party service providers, or subcontractors that need it to provide the contracted services.

(e) Vendor will not use Education Records or PII for any purpose other than those explicitly authorized in the Full Agreement. Without limiting the foregoing, Vendor will not use Protected Data to train, fine-tune, or improve any AI or machine-learning model beyond the scope of the contracted services.

(f) Except for authorized representatives of Vendor (such as a subcontractor, third-party service provider, or assignee) carrying out the Full Agreement in compliance with law, Vendor will not disclose PII to any other party unless: (i) the disclosure is to an authorized representative of Vendor identified in Section 6 of Exhibit A, is necessary to carry out the Full Agreement, and is limited to the Protected Data elements identified for that representative in that schedule; (ii) the Parent or Eligible Student has provided prior written consent; or (iii) the disclosure is required by statute or court order and Vendor provides notice to the District no later than the time of disclosure, unless expressly prohibited.

(g) Vendor shall maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody. Vendor's safeguards, technologies, and practices align with the NIST Cybersecurity Framework, the standard adopted under 8 NYCRR § 121.5. Protected Data at rest in Vendor's database, and the backups of that database, are held in United States regions, and Vendor operates no store, no backup, and no personnel access path outside the United States; Vendor does not warrant that no Protected Data ever leaves the United States, because certain of its subprocessors do not give Vendor that warranty; the specific providers and the limitation each imposes are enumerated in DPA § 3.7 and Exhibit A § 5, and this paragraph incorporates that disclosure by reference.

(h) Vendor will protect PII in its custody in motion and at rest using encryption technology that complies with NY 2-d. Specifically, Vendor uses provider-managed storage/volume-level encryption at rest and TLS 1.2 or higher in transit, with application-level envelope encryption (AES-256-GCM with RSA-OAEP key wrapping)

applied to school-system credentials held on the Platform. Vendor does not represent that its database provider uses customer-managed page-level BYOK encryption; encryption at rest is the provider's managed volume-level encryption.

(i) Vendor and its personnel and assignees with access to Protected Data have received or will receive training on the federal and state laws governing confidentiality of Protected Data, and have completed or will complete a criminal background check, in each case prior to receiving access and at least annually thereafter. A formal criminal background check has been performed.

(j) Vendor will not collect or retain any Protected Data beyond what is necessary to provide the services (data minimization). Vendor is expressly prohibited from collecting or retaining: Social Security Numbers, student grades or academic records, full IEP documents or disability classifications, medical or behavioral-health records, immigration or citizenship status, financial-aid eligibility, student photographs or biometric data, disciplinary records, or religion/ethnicity/race/national-origin data.

3. DELETION OR DISPOSITION OF PROTECTED DATA UPON TERMINATION

The consent and revocation record described in DPA § 3.1(a) is excepted from this Section. That record is retained for four (4) years after the engagement ends in accordance with DPA § 9, reduced at termination to the telephone number, the email address, the suppression status, the consent status, the version of the consent wording shown, the capture method and timestamp, and the date, method and channel of any revocation; it is used for no purpose other than evidencing compliance with 47 CFR § 64.1200 and responding to a regulatory inquiry or claim. **This exception controls over the general deletion obligation in this Section and over Exhibit A § 9.** Subject to that exception, within **thirty (30) days** of the expiration of the Full Agreement without renewal, or its termination prior to expiration, Vendor will securely delete or destroy all Protected Data remaining in its possession and instruct its subcontractors or other authorized entities to securely delete or destroy all Protected Data in their possession within **ninety (90) days** of termination. **Redaction is not an acceptable means of destruction; destruction must render Protected Data permanently unreadable and unrecoverable.** At the District's option and direction, Vendor will alternatively transition Protected Data to a District-designated successor contractor that has executed data-protection agreements no less protective than this Addendum. Upon request, Vendor will provide the District with written certification from an authorized officer confirming these deletion or transition requirements have been satisfied in full.

4. DATA SECURITY AND PRIVACY PLAN

Vendor maintains a Data Security and Privacy Plan complying with NY 2-d and 8 NYCRR § 121.6 (the "Vendor Plan"), attached as **Exhibit A** and incorporated herein. Vendor will provide an updated Vendor Plan to the District upon written request and in advance of any material change to Vendor's data-security practices. **By executing this Addendum the District accepts the Vendor Plan as the third-party contractor's plan required by 8 NYCRR § 121.6.** The District supplies Vendor, before execution, with the data security and privacy policy the District has adopted under 8 NYCRR § 121.5, and Vendor's acceptance of this Addendum includes its agreement to comply with that policy as required by 8 NYCRR § 121.9(a)(2). Where the District's

policy imposes a requirement stricter than the Vendor Plan, the District's policy governs and Vendor will conform the Vendor Plan to it or state in writing that it cannot, in which case the District may terminate this Addendum without penalty.

5. SUBCONTRACTORS

Where Vendor engages subcontractors, third-party service providers, or other authorized entities to perform its obligations (including hosting), Vendor will require those to whom it discloses Protected Data to execute legally binding agreements providing security and confidentiality no less stringent than the obligations required of Vendor in this Addendum. Vendor remains responsible for compliance and is liable to the District for the acts and omissions of any such party as if they were Vendor's own. A complete, current list of subcontractors with access to Protected Data is in **Section 6 of Exhibit A**, which reproduces DPA § 5.3(a); DPA § 5.3(a) controls on any difference. The current schedule is published at **schools.askelira.com/legal/subprocessors** and changes only on the notice DPA § 5.3 requires. Vendor will provide the District with at least **thirty (30) days'** advance written notice before adding or replacing any subcontractor with access to Protected Data.

6. NOTIFICATION OF BREACH AND UNAUTHORIZED RELEASE

(a) Vendor shall promptly notify the District of any Breach or Unauthorized Release of Protected Data by Vendor or its assignees (an "Incident") in the most expedient way possible and without unreasonable delay, but **no more than forty-eight (48) hours** after discovery — a contractual commitment stricter than, and in no event later than, the seven (7) calendar days permitted for contractor-to-agency notice by 8 NYCRR § 121.10(a). Notifications shall be plain and clear and, to the extent available, include: a brief description of the Incident; the dates of the Incident and of discovery, if known; the types of Protected Data affected; an estimate of the number of records affected; a brief description of Vendor's investigation or plan to investigate; and contact information for AskElira representatives who can assist Parents or Eligible Students. Vendor will notify the District's designated Data Protection Officer by email, with a copy to the authorized representative in the signature block.

(b) Vendor will cooperate with the District and law enforcement to protect the integrity of the investigation and will preserve all relevant evidence for forensic purposes.

(c) This obligation is not subject to any limitation of liability in the Full Agreement, and no cap in MSA § 11 or DPA § 12.3 applies to it. Where an Incident is attributed to Vendor within the meaning of 8 NYCRR § 121.10(f), Vendor shall pay or promptly reimburse the District for the full reasonable and documented cost of notifications required under NY 2-d to affected Parents, Eligible Students, teachers, and/or principals, including costs of required regulatory reporting to the NYSED Chief Privacy Officer.

(d) Vendor acknowledges that upon initial notification, the District has a separate obligation under NY 2-d and 8 NYCRR § 121.10(b) to notify the NYSED Chief Privacy Officer ("CPO") no more than ten (10) calendar days after receiving Vendor's notification, and to notify affected parents, eligible students, teachers, and principals no more than sixty (60) calendar days **after the discovery of the breach or unauthorized release** (§ 121.10(e)). **That sixty-day period runs from discovery, not from the District's receipt of Vendor's notice**, so any time Vendor takes to notify is time deducted from the District's own period. Vendor's 48-hour commitment under subsection (a) — against the seven calendar days § 121.10(a) permits — exists to preserve as much of the District's statutory period as possible. Vendor will not notify the CPO directly unless expressly requested by the District or required by law. If the CPO contacts Vendor directly after being informed by the

District, Vendor will promptly inform the District's Data Protection Officer before responding. Vendor further acknowledges that, following any confirmed Unauthorized Disclosure, the CPO is authorized to require Vendor to provide retraining at Vendor's expense to all officers and employees with access to Protected Data, and Vendor agrees to comply.

7. PARENTS' BILL OF RIGHTS

(a) The District's Bill of Rights is attached and controls. As required by 8 NYCRR § 121.3(b), the District's own adopted and published Parents' Bill of Rights for Data Privacy and Security is included with this contract and is attached as **Annex 1** to this Addendum. The District's adopted document governs; nothing AskElira has drafted substitutes for it. By executing this Addendum, Vendor signs and acknowledges the District's Parents' Bill of Rights and will comply with it as required under NY 2-d. **Attachment of Annex 1 is a condition precedent to the effectiveness of this Addendum.** If Annex 1 has not been attached, this Addendum does not take effect, the Full Agreement does not authorize any Processing of Protected Data, and no Protected Data will be connected to the Platform. **Annex 1 may be attached at or after execution.** The District attaches its published document through its AskElira account, and this Addendum takes effect on the date of that attachment. AskElira records the file name, a SHA-256 digest of the file, the date and time of attachment, and the account that attached it; that record is the evidence of attachment for § 121.3(b) purposes and is available to the District on request. Until the attachment is recorded, AskElira does not connect to the District's student information system, reads no roster, and contacts no family — a state the District can see in its own account at any time. The District may replace the attached document at any time; the record retains each prior version and the date it was superseded.

Annex 1 — attached by the District

Annex 1: the District's adopted Parents' Bill of Rights for Data Privacy and Security. The District attaches its published document through its AskElira account, at or after execution. This Addendum is not complete for § 121.3(b) purposes, and does not take effect, until it is attached. The attachment record — file name, SHA-256 digest, date and attaching account — is maintained by AskElira and is the evidence of attachment. A District that prefers to attach a paper copy to this instrument at execution may do so, and should note the file name below.

District confirms attachment — initials: _____ date: _____

(b) The supplement is the District's document. Under 8 NYCRR § 121.3(c) the supplemental information for this contract **must be developed by the educational agency**, and under § 121.3(d) the District publishes it on its website. **Exhibit B** is AskElira's vendor-side content for each of the six required items, supplied so the District can develop and publish its supplement; it is not itself the District's supplement, and AskElira does not purport to develop it. Vendor will supply any further information the District requires to complete it, and will cooperate with the District's § 121.8 Data Protection Officer in fulfilling all obligations under this Addendum and NY 2-d.

8. PARENT AND ELIGIBLE STUDENT RIGHTS

Parents, legal guardians, and eligible students (18 or older) may challenge the accuracy of Protected Data held by Vendor by contacting the District in accordance with the District's procedures for requesting amendment to education records under FERPA. Vendor will work with the District in processing challenges and will correct or flag disputed data within **three (3) business days** of a verified written request from the District.

9. COVERED THIRD-PARTY CONTRACTOR ACKNOWLEDGMENT AND REGULATORY COMPLIANCE

(a) Vendor acknowledges it is a "third-party contractor" under NY Education Law § 2-d and 8 NYCRR Part 121, subject to the jurisdiction, oversight, and enforcement authority of the NYSED Chief Privacy Officer, and agrees to cooperate with any CPO investigation, inspection, or audit.

(b) Vendor acknowledges the civil penalties in 8 NYCRR § 121.11: failure to notify the educational agency of a breach resulting in an unauthorized release is punishable by a civil penalty of **the greater of $5,000 or up to $10 per affected student, teacher, and principal**, capped at the maximum under General Business Law § 899-aa(6)(a) (§ 121.11(a)); any other violation of Education Law § 2-d is punishable by a civil penalty of **up to $1,000**, rising to up to $5,000 for a second violation involving the same data and up to $10,000 for any subsequent violation involving the same data, each violation counting separately and subject to the same statutory cap (§ 121.11(b)). Vendor further acknowledges that, following a determination and the thirty-day response opportunity under § 121.11(d), the Chief Privacy Officer may, under § 121.11(e)(1)–(4), preclude Vendor from accessing personally identifiable information from the affected educational agency for up to five (5) years, may preclude a Vendor that knowingly or recklessly allowed the release from accessing such data from **any** educational agency in the State for up to five (5) years, may render Vendor a non-responsible bidder for up to five (5) years, and may require additional training at Vendor's expense. Vendor represents that it has implemented the safeguards in this Addendum and the Full Agreement specifically to avoid such violations.

(c) If the CPO determines Vendor committed an Unauthorized Disclosure and orders remedial action, Vendor will comply, including providing retraining at its expense to all officers and employees with access to Protected Data, and will report compliance to both the CPO and the District within the timeframe specified.

EXECUTION

IN WITNESS OF THE FOREGOING, the duly authorized representatives have signed this Addendum as of the Effective Date.

stoplosses.ai LLC, a Wyoming limited liability company

SIGNATURE DATE

ALVIN KERREMANS · CHIEF EXECUTIVE OFFICER AND SOLE MEMBER · AUTHORIZED TO BIND STOPLOSSES.AI LLC

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.

EXHIBIT B — VENDOR CONTENT FOR THE DISTRICT'S § 121.3(c) SUPPLEMENT

Third-Party Contractor: stoplosses.ai LLC ("Vendor") · **Educational Agency:** `{{school_name}}` (the "District")

Whose document this is

Under 8 NYCRR § 121.3(c) the supplemental information for this contract **must be developed by the educational agency**, and under § 121.3(d) the District publishes it on the District's website. This Exhibit is Vendor's content for each of the six required items, supplied so the District can develop and publish its supplement. It is not the District's supplement, and it is not the District's Parents' Bill of Rights — that document is attached to this Addendum as Annex 1 under § 121.3(b). Item (3) requires the contract's expiration date, which comes from the executed Order Form and is completed below by the District.

COMPLETED BY THE DISTRICT FROM THE EXECUTED ORDER FORM

Contract expiration date *(§ 121.3(c)(3))*	_____
District Data Protection Officer *(§ 121.8)*	_____

Terms have the meanings given in NY § 2-d. "Protected Data" means student data and/or teacher or principal data as defined in NY § 2-d.

(1) Exclusive purposes for which the data will be used. AskElira uses Protected Data solely to provide enrollment- and attendance-automation services on behalf of the District. This includes: email and SMS outreach sequences to families of offered/accepted/declined/waitlisted applicants; **automated enrollment voice calls delivered as a deterministic keypad-response IVR** (Monday–Friday, in Eastern Time — a morning window 9:00 AM–12:00 PM, an early-evening follow-up window 5:00–6:30 PM for non-responders, and an early-afternoon window 1:00–4:00 PM, one attempt per window, up to three attempts) — **these calls are not recorded and not transcribed; only the call outcome and a brief summary are retained**; same-day attendance notifications to guardians of absent students, and — **only where the School switches it on** — a late-arrival (tardy) notice to guardians of students marked late, sent as **one bilingual text message and nothing else**, no automated call and no email, no more than once per student per school day, and never enabled for a School whose captured consent language does not disclose it — **text and email notices name the student in full** so a household with more than one child knows which child is meant, while **voice announcements say the first name only** because a call plays to whoever answers — each voice announcement offering a keypad option (press 6) that stops further automated attendance calls while the text and email notices continue — reversible at any time by texting the word CALLS from that number — alongside the same press-7 wrong-number key, press-8 stop-everything key, and press-9 main-office key that every automated call carries — with permanent suppression of any number reported as a wrong number; IEP-director notification on Day 1 of each enrollment sequence; a daily enrollment digest email to the school's operations team; enrollment-tracker (Google Sheets) autofill; the family question-and-answer assistant, which answers guardian questions submitted through the School's website chat widget, by inbound text message, or — where the School enables that channel — by inbound WhatsApp message, grounded in the School's own published content; and an automated send-or-hold review of Staff Enrollment Notes before an outbound message is released. Both of those last two functions are performed by the AI model provider or providers named in DPA §

5.3(a) and Section 6 of Exhibit A, each on a US Processing Endpoint, and neither is used to train or improve any model. AskElira also receives registration documents that families email the School's office — it identifies which required document arrived from the file name, forwards it to School staff, and records on the checklist that it was received and forwarded. **No document is opened, read, stored, or sent to an AI model**; confirming a document is the right one for the right child is School staff's judgement, in the School's own system. Protected Data is used for no other purpose. AskElira will not sell PII, will not use or disclose it for any marketing or commercial purpose, and will not use Protected Data to train, fine-tune, or improve any AI/ML model beyond the scope of services.

(2) How subcontractors will abide by data-protection requirements. AskElira limits access to Protected Data to employees, subcontractors, and service providers with a legitimate need to deliver the services. All personnel with access receive training on applicable federal and state privacy laws (NY 2-d, FERPA, COPPA, IDEA) before access and annually. AskElira requires every subcontractor that receives Protected Data to be bound by written data-protection terms covering confidentiality, security, breach notification, and deletion on AskElira's instruction, and remains fully responsible to the District for its subcontractors' handling of Protected Data. Where a provider publishes standard terms that AskElira cannot negotiate, AskElira imposes on each subprocessor, by written agreement, data-protection obligations no less protective than those AskElira owes the District, 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 District switches it on**, and why leaving it off costs the District nothing else in the Services. Any provider referred to in DPA § 3.5 is marked as an AI model provider in the DPA § 5.3(a) schedule and in Section 6 of Exhibit A; where more than one is listed, each is engaged only for the functions stated for it there. AskElira's subcontractors with access to Protected Data are, as stated in DPA § 5.3(a) as of Version 3.0 · August 2026: **Twilio** (SMS and keypad-IVR/TTS voice, and the WhatsApp Business API through which the WhatsApp channel is reached), **Meta Platforms** (the WhatsApp network itself, where the School enables WhatsApp as a channel for the family question-and-answer assistant — Meta receives the guardian's question and the assistant's answer, and gives AskElira no United States processing commitment, as stated in item (5) below), **Google Cloud** (Vertex AI — family Q&A assistant, staff support, and the reading of School-published documents such as flyers and calendars, on a US Processing Endpoint; content is not used to train Google's models — and Google Sheets), **Amazon Web Services** (Amazon Bedrock — the staff-note send/hold review, on a US Processing Endpoint at zero data retention with zero operator access; the model it serves was developed by DeepSeek and is operated entirely by AWS inside AWS's United States infrastructure, the developer receives no content, and content is not used to train any model), **Turso** (database), **Vercel** (hosting and runtime), **AgentMail/Amazon SES** (email delivery and inbound authentication), **Resend** (standby outbound email delivery, used only where the primary provider will not accept a message for transport), and **SchoolMint** (school-authorized enrollment-system integration). *(Anthropic is internal development tooling only and receives no Protected Data. The former conversational-voice path, which used VAPI with OpenAI as its model provider, was retired on July 24, 2026.)* The complete, current list is in DPA § 5.3(a) and Section 6 of Exhibit A, and is published at **schools.askelira.com/legal/subprocessors**, where a parent or the District can read it at any time without asking for the contract; the District receives at least **30 days'** notice before any subcontractor is added or replaced, and an opportunity to object.

(3) Contract duration, expiration date, and data disposition. The term and the expiration date are stated in the District's executed Order Form to the Master SaaS & Services Agreement and are entered in the table at the head of this Exhibit. Annual packages run 12 months and auto-renew in 12-month terms unless either party gives 30 days' notice of non-renewal; the Seasonal package runs its committed period (4-month minimum) and expires without renewing. The agreement remains in force for the District's active subscription and renews concurrently unless terminated. Because NYC charter schools enroll year-round, Protected Data is retained while the subscription is active. **One category outlives the contract and families should know it:** the consent, opt-out and wrong-number suppression records are kept for the engagement plus four (4) years, reduced at termination to the telephone number, email address, suppression status and date. That is deliberate — deleting a suppression record would put a number a family asked us never to call back into contactable status, and the record is what evidences compliance with 47 CFR § 64.1200 past the limitations period for a claim. Everything else follows the schedule below; independently of contract end, guardian and student personal data that has gone inactive is automatically deleted after **90 days** under the DPA. Within **30 days** of expiration without renewal, or termination, AskElira securely deletes all remaining Protected Data and instructs subcontractors to do the same within **90 days**. Redaction is not acceptable destruction. At the District's option, AskElira will transition Protected Data to a District-designated successor in lieu of deletion. Written certification is provided on request.

(4) How to challenge accuracy. A parent or eligible student may challenge the accuracy of Protected Data by contacting the District's Data Protection Officer under the District's FERPA amendment procedures; AskElira corrects or flags disputed data within **3 business days** of a verified written request from the District.

(5) Where data is stored and how protected. AskElira'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 AskElira-operated store or backup outside the United States. Authorized AskElira 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. **AskElira 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. Safeguards include TLS 1.2+ in transit, provider-managed storage/volume-level AES-256 encryption at rest, application-level envelope encryption for school-system credentials, role-based access control, multi-factor administrative sign-in enforced on every account (a per-user password held only as a salted cryptographic digest, plus a single-use link emailed to that person), security-event logging, and NIST-CSF-aligned controls, with automated around-the-clock

monitoring and a 48-hour breach-notice operational standard — well inside the seven-calendar-day maximum for contractor-to-agency notice under 8 NYCRR § 121.10(a). The AI functions described in item (1) are core Platform functionality and are not offered on an opt-out basis.

(6) Encryption in motion and at rest. TLS 1.2 or higher in transit (TLS 1.3 at the public edge); provider-managed storage/volume-level AES-256 encryption at rest; school-system credentials additionally protected with application-level envelope encryption (AES-256-GCM with RSA-OAEP key wrapping). These measures comply with the encryption requirements of NY § 2-d and 8 NYCRR Part 121.

[End of Addendum, Exhibit A, and Exhibit B]

---

stoplosses.ai LLC · 3660 Oxford Ave, Bronx, NY 10463 · akerremans@askelira.com · Part of the AskElira Schools onboarding packet (v2.7, August 2026). The executed MSA, DPA, and NY Ed Law § 2-d Addendum control over any summary of them.