

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.