NEW YORK PRIVATE SCHOOL DATA SECURITY AND PRIVACY ADDENDUM

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

Including **Exhibit A** (Data Security and Privacy Plan, incorporated by reference) and **Exhibit B** (Family Data Rights Statement, supplied for the School to adopt and publish).

PARTIES TO THIS ADDENDUM

School	`{{school_name}}` (the "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 New York Private School Data Security and Privacy Addendum ("Addendum") is entered into by `{{school_name}}` (the "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. **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 Agreement and this Addendum are collectively the "Full Agreement."

Why this instrument exists, and why it is not the § 2-d Addendum. New York Education Law § 2-d and Part 121 of the Commissioner's Regulations impose duties on an "educational agency" — a school district, board of cooperative educational services, or charter school — and on the third-party contractors that receive protected data from one. **A private or independent school is not an educational agency within that definition, so § 2-d and Part 121 do not govern this engagement.** The School therefore executes this Addendum in place of, and not in addition to, the NY Education Law § 2-d Addendum that appears in the packet issued to public and charter schools. What governs instead is stated in § 9 below: the New York SHIELD Act, the Children's Online Privacy Protection Act where a child under 13 is involved, the Telephone Consumer Protection Act, and the contractual commitments in this Addendum. Where this Addendum imposes a duty on Vendor that no statute imposes, that duty is a contractual promise the School may enforce as such.

1. DEFINITIONS

(a) As used herein, **"Protected Data"** means the personal information of a student or of a student's parent or guardian that the School discloses to Vendor, or that Vendor collects on the School's behalf, in each case in connection with the Full Agreement, 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 or report-card grade); seat, application or admission status (inquired, toured, applied, 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); 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**); **family 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 family 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.

(b) "Private Information" has the meaning given in N.Y. General Business Law § 899-aa(1)(b). Protected Data may include Private Information; where it does, the obligations of this Addendum apply in addition to, and not in place of, Vendor's obligations under the SHIELD Act.

(c) "Security Incident" means a breach of the security of the system within the meaning of N.Y. General Business Law § 899-aa(1)(c), or any other unauthorized acquisition of, access to, or disclosure of Protected Data in Vendor's custody.

(d) Terms not defined here have the meanings given in the Master SaaS & Services Agreement or the Data Processing Agreement.

2. VENDOR'S OBLIGATIONS AND CONFIDENTIALITY

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

(b) Vendor will maintain the confidentiality of Protected Data in accordance with applicable federal and state law, including the SHIELD Act and, where a child under 13 is involved, COPPA, and in accordance with the School's own written data security and privacy policy where the School has adopted one and supplied it to Vendor in writing.

(c) Vendor will not sell Protected Data 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 Protected Data to those employees, third-party service providers, and subcontractors who need it to provide the contracted services.

(e) Vendor will not use Protected Data 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 Protected Data to any other party unless: (i) the disclosure is to an authorized representative of Vendor identified in the subprocessor schedule described in § 5, 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, guardian, 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 School 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 Protected Data in its custody, as required by N.Y. General Business Law § 899-bb(2). Vendor's safeguards, technologies, and practices align with the NIST Cybersecurity Framework. 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 this paragraph incorporates that disclosure by reference.

(h) Vendor will protect Protected Data in its custody in motion and at rest using encryption technology no weaker than the following: provider-managed storage and volume-level encryption at rest, TLS 1.2 or higher in transit, and 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 or award amounts, tuition payment or family financial records, student photographs or biometric data, disciplinary records, or religion, ethnicity, race, or 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.** 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 School's option and direction, Vendor will alternatively transition

Protected Data to a School-designated successor contractor that has executed data-protection agreements no less protective than this Addendum. Upon request, Vendor will provide the School with written certification from an authorized officer confirming these deletion or transition requirements have been satisfied in full.

Routine retention during the engagement. Independently of termination, Vendor purges the personal data of a family ninety (90) days after that family's record goes inactive, as stated in DPA § 9 and as enforced by the retention job described in Exhibit A.

4. DATA SECURITY PROGRAM — SHIELD ACT § 899-bb(2)

(a) The Plan. Vendor maintains a written Data Security and Privacy Plan (the "Vendor Plan"), which is **Exhibit A** to this Addendum and is incorporated herein by reference. Vendor will provide the current Vendor Plan to the School upon written request and in advance of any material change to Vendor's data-security practices.

(b) The statutory elements. The Vendor Plan implements a data security program containing reasonable administrative, technical and physical safeguards, addressing each element listed in N.Y. General Business Law § 899-bb(2)(b). The table below maps each statutory element to the section of the Vendor Plan that implements it, so the School can verify coverage without reading the whole Plan.

SHIELD ACT PROGRAM ELEMENTS AND WHERE EACH IS IMPLEMENTED

Statutory element	§ 899-bb(2)(b)	Vendor Plan section
Designates one or more employees to coordinate the security program	(A)(1)	§ 1, § 8.2
Identifies reasonably foreseeable internal and external risks	(A)(2)	§ 8.1, § 8.3
Assesses the sufficiency of safeguards in place to control the identified risks	(A)(3)	§ 8.3
Trains and manages employees in the security program practices and procedures	(A)(4)	§ 7
Selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract	(A)(5)	§ 6
Adjusts the security program in light of business changes or new circumstances	(A)(6)	§ 2, § 8.3
Assesses risks in network and software design	(B)(1)	§ 3.2
Assesses risks in information processing, transmission and storage	(B)(2)	§ 3.2, § 5
Detects, prevents and responds to attacks or system failures	(B)(3)	§ 8.1, § 8.2
Regularly tests and monitors the effectiveness of key controls, systems and procedures	(B)(4)	§ 8.1, § 8.3
Assesses risks of information storage and disposal	(C)(1)	§ 3.4, § 9
Detects, prevents and responds to intrusions	(C)(2)	§ 8.1
Protects against unauthorized access to or use of private information during or after collection, transportation and destruction or disposal	(C)(3)	§ 3.2, § 3.4, § 9

Statutory element	§ 899-bb(2)(b)	Vendor Plan section
Disposes of private information within a reasonable amount of time after it is no longer needed, so that it cannot be read or reconstructed	(C)(4)	§ 9

(c) No certification is claimed. The Vendor Plan is a plan, not a certification. Vendor does not hold and does not claim a SOC 2 report, an ISO 27001 certificate, or any third-party security certification, and nothing in this Addendum may be read as such a claim.

(d) The School's own policy governs where it is stricter. Where the School has adopted a written data security and privacy policy and supplied it to Vendor, and that policy imposes a requirement stricter than the Vendor Plan, the School's policy governs and Vendor will conform the Vendor Plan to it or state in writing that it cannot, in which case the School 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, as N.Y. General Business Law § 899-bb(2)(b)(A)(5) requires. Vendor remains responsible for compliance and is liable to the School for the acts and omissions of any such party as if they were Vendor's own. **The authoritative, current schedule of subcontractors with access to Protected Data is published at schools.askelira.com/legal/subprocessors**, and DPA § 5.3(a) controls on any difference between that page and any printed copy. Vendor will provide the School with at least **thirty (30) days'** advance written notice before adding or replacing any subcontractor with access to Protected Data.

6. NOTIFICATION OF A SECURITY INCIDENT

(a) Vendor shall notify the School of any Security Incident affecting Protected Data in Vendor's custody in the most expedient way possible and without unreasonable delay, but **no more than forty-eight (48) hours** after discovery. Notifications shall be plain and clear and, to the extent available, include: a brief description of the Security Incident; the dates of the Security 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 affected families.

(b) Vendor will cooperate with the School and with 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 a Security Incident is attributable to Vendor, Vendor shall pay or promptly reimburse the School for the full reasonable and documented cost of the notifications the School is required to make to affected New York residents under N.Y. General Business Law § 899-aa, and of any regulatory notification that section requires the School to make.

(d) The School's own statutory duty. Vendor acknowledges that where Protected Data includes Private Information of a New York resident, the School has its own obligation under N.Y. General Business Law § 899-aa to notify affected individuals in the most expedient time possible and without unreasonable delay, and to notify the New York State Attorney General, the Department of State, and the Division of State Police. Vendor's 48-hour commitment under subsection (a) exists to preserve as much of the School's own response time as possible. Vendor will not make a notification to a regulator or to a family in the School's name unless the School expressly requests it in writing or the law requires Vendor to do so directly.

7. FAMILY DATA RIGHTS STATEMENT

(a) What Exhibit B is. Exhibit B is the Family Data Rights Statement: a plain-language statement of what AskElira does with a family's data, what it never does, how long it keeps it, and how a family reaches a person. It is supplied by Vendor for the School to adopt and publish. Unlike the Parents' Bill of Rights that 8 NYCRR § 121.3 requires of a public or charter school, **no statute requires a private school to publish this statement.** It is offered because a family that can read what happens to its data complains less and consents more knowingly, and because the School may be asked for it by an accrediting body or by a family.

(b) The School decides. The School may publish Exhibit B as supplied, edit it, replace it with its own statement, or publish nothing. Publication is **not** a condition of this Addendum taking effect and **not** a condition of service. Where the School publishes an edited version, the School is responsible for its accuracy about the School's own practices; Vendor remains responsible for the accuracy of what Exhibit B says about Vendor.

(c) What Vendor will not do. Vendor will not represent to any family, accrediting body, or regulator that the School has published a family data rights statement unless the School has told Vendor in writing that it has.

8. FAMILY AND STUDENT RIGHTS

(a) Correction. A parent, legal guardian, or student aged 18 or older may challenge the accuracy of Protected Data held by Vendor by contacting the School. Vendor will work with the School in processing such challenges and will correct or flag disputed data within **three (3) business days** of a verified written request from the School.

(b) Access and deletion. On the School's verified written request, made on behalf of a family, Vendor will provide the School with a copy of the Protected Data Vendor holds about that family, or delete it, within **ten (10) business days**. Vendor takes instructions about a family's data from the School and not from the family directly, because the School — not Vendor — holds the relationship and can verify who is asking.

(c) Communications opt-out is immediate and permanent. Independently of subsection (b), a family may stop AskElira communications at any time by replying STOP to a text message, using the unsubscribe link in an email, or telling the School. An opt-out is honoured on the channel it is given, is permanent, and is not undone by a later data upload from the School. The consent and revocation record described in DPA § 3.1(a) is what makes that permanence provable.

(d) COPPA. Where the Platform collects personal information online from a child under 13, Vendor relies on the School to provide consent as the parent's agent for the limited educational purpose of the Full Agreement, in accordance with the Federal Trade Commission's guidance on school consent under 16 CFR Part 312. Vendor

does not condition a child's participation on the disclosure of more personal information than is reasonably necessary, and does not use such information for any commercial purpose.

9. REGULATORY POSITION AND ACKNOWLEDGMENTS

(a) Education Law § 2-d does not apply. Vendor and the School acknowledge that the School is not an "educational agency" within the meaning of N.Y. Education Law § 2-d(1)(a), that Vendor is therefore not a "third-party contractor" of the School within the meaning of § 2-d(1)(i) by reason of this engagement, and that 8 NYCRR Part 121 does not govern it. **The School represents that it is a private or independent school and is not a school district, board of cooperative educational services, or charter school.** If that representation ceases to be accurate, the School will tell Vendor in writing, and the parties will replace this Addendum with the NY Education Law § 2-d Addendum, which Vendor will supply.

(b) FERPA. The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, applies to an educational agency or institution that receives funds under a program administered by the U.S. Department of Education. **The School represents whether it receives such funds by ticking one box below.** Where the School does receive them, Vendor will act as a school official with a legitimate educational interest under 34 CFR § 99.31(a)(1), will use Protected Data only for the purposes authorized in the Full Agreement, will not redisclose it except as this Addendum permits, and will remain under the School's direct control with respect to the use and maintenance of education records. Where the School does not receive them, FERPA does not govern this engagement, and the commitments in this paragraph nonetheless apply **as a matter of contract**, enforceable by the School as though FERPA applied.

The School receives U.S. Department of Education program funds — Yes _____ No _____

(c) SHIELD Act enforcement. Vendor acknowledges that N.Y. General Business Law §§ 899-aa and 899-bb are enforced by the New York State Attorney General, and that a failure to maintain reasonable safeguards or to give required notice may result in civil penalties and injunctive relief. Vendor represents that it has implemented the safeguards in this Addendum, the Vendor Plan, and the Full Agreement specifically to avoid such violations.

(d) TCPA. Automated contact with families is governed by the Telephone Consumer Protection Act, 47 U.S.C. § 227, and 47 CFR § 64.1200, on exactly the same terms as for a public school. The consent pathways, the New York school-day calling window, the caller identification and callback number, and the opt-out handling are stated in the TCPA Consent & Outreach Scripting document and the Guardian Consent Language document, both of which are contract documents under MSA § 14.12.

(e) Accreditation and independent-school associations. Nothing in this Addendum satisfies, replaces, or speaks to a requirement imposed on the School by an accrediting body or an independent-school association. The School is responsible for its own accreditation obligations, and Vendor will supply information the School reasonably needs to meet them.

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

School — `{{school_name}}`

SIGNATURE | DATE

PRINTED NAME | TITLE

EXHIBIT A — ASKELIRA DATA SECURITY AND PRIVACY PLAN

This Exhibit A is the AskElira Data Security and Privacy Plan, the same document AskElira publishes at **schools.askelira.com/legal** as the Information Security Policy and supplies to every school it serves. **It is incorporated into this Addendum by reference and forms part of it.** It is incorporated rather than reprinted for one reason: there is one Plan, and a printed copy inside a signed contract becomes a second version of it the moment the Plan is updated. The section numbers used in the mapping table at § 4(b) of this Addendum are the section numbers of that Plan.

The Plan is written against 8 NYCRR § 121.6, which does not apply to the School. It is supplied unchanged rather than rewritten, because the safeguards it describes are the safeguards AskElira actually runs, and describing the same safeguards twice in two documents is how two documents start to disagree. Where the Plan refers to an educational agency, a district, or Part 121, read those references as referring to the School and to this Addendum.

Vendor will notify the School in writing at least thirty (30) days before a material change to the Plan, and the version of the Plan in force on the Effective Date is available to the School on request as a dated PDF for its own records.

EXHIBIT B — FAMILY DATA RIGHTS STATEMENT

This Exhibit B is supplied for the School to adopt and publish under § 7 of this Addendum. No statute requires a private school to publish it. It is written in the second person, addressed to a family, so that it can be published as it stands.

Your family's data, and what AskElira does with it

`{{school_name}}` uses AskElira, a service run by stoplosses.ai LLC, to answer admissions questions, schedule tours, send reminders about applications and enrollment, and — where the School uses it — tell you the same day if your child is marked absent.

(1) What is collected. Your name, phone number, email address, and preferred language; your child's first name, and full name where a message names the student; grade level; application or admission status; where the School uses attendance alerts, one attendance category per school day; the questions you ask AskElira; and a record of each message sent to you and what happened to it. A full list is in § 1 of the addendum the School signed with AskElira.

(2) What is never collected. Social Security numbers, grades and academic records, disability classifications or IEP documents, medical and behavioural-health records, immigration status, financial-aid or tuition-payment records, photographs and biometrics, disciplinary records, and religion, ethnicity, race or national origin.

(3) What it is used for, and what it is never used for. Your data is used to run the School's admissions and enrollment communications, and for nothing else. It is **never sold**. It is **never used for advertising or marketing**. It is **never used to train an AI model**.

(4) Who else sees it. A small number of named service providers — for hosting, email, text messaging, and AI processing — see the data they need to do their part, under contracts no less protective than the School's. The current list is published at **schools.askelira.com/legal/subprocessors** and changes only after thirty days' notice to the School.

(5) Where it is held. Data at rest is held in United States regions, and there is no store, backup or staff access path outside the United States. AskElira does not promise that no data ever crosses the border, because some of its providers do not give AskElira that promise. The specific providers and the specific limitation each imposes are named in the published subprocessor list.

(6) How long it is kept. Ninety (90) days after your family's record goes inactive, personal data is purged. One record outlives that: if you gave or withdrew consent to be contacted, the proof of that — your number or address, the wording you were shown, and the date — is kept for four years, and used only to show a regulator that the rules were followed.

(7) How to stop the messages. Reply STOP to any text. Use the unsubscribe link in any email. Or tell the School. Stopping is immediate, permanent, and is not undone by a later upload from the School.

(8) How to see, correct, or delete your data. Ask the School. The School verifies who you are — AskElira does not, because the School holds the relationship. AskElira corrects or flags disputed data within three business days of the School's request, and provides a copy or deletes it within ten business days.

(9) If something goes wrong. If family data held by AskElira is exposed, AskElira must tell the School within forty-eight hours of discovering it, and must pay the cost of the notices the School then has to send.

(10) Who to contact. Write to the School's admissions office, or to AskElira's privacy contact at **privacy@askelira.com**.

---

stoplosses.ai LLC · 3660 Oxford Ave, Bronx, NY 10463 · This statement forms part of the AskElira Schools Onboarding Packet and is published at schools.askelira.com/legal.