STUDENT DATA PRIVACY ADDENDUM

Exhibit G — Educational Institutions

Version 1.3

H&A Security Solutions, LLC d/b/a Tellaro — 12178 N 1450th Street, Effingham, Illinois 62401

STUDENT DATA PRIVACY ADDENDUM

This Student Data Privacy Addendum (this "Addendum") is Exhibit G to the Master Subscription Agreement or the End User License Agreement — On-Prem, as applicable (the "Agreement"), between H&A Security Solutions, LLC, an Illinois limited liability company doing business as Tellaro ("Tellaro"), and the customer identified on the signature page ("Customer"). It applies when Customer is an Educational Institution and Customer Data includes Student Data. Capitalized terms not defined here have the meanings given in the Agreement and the Data Processing Addendum (the "DPA"). With respect to Student Data, this Addendum controls over any conflicting term of the Agreement or the DPA.

1. DEFINITIONS

"Applicable Student Privacy Laws" means the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and 34 C.F.R. Part 99 ("FERPA"); the Protection of Pupil Rights Amendment, 20 U.S.C. § 1232h; the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506, to the extent applicable; the Illinois Student Online Personal Protection Act, 105 ILCS 85 ("SOPPA"); and any other state student-privacy law that applies to Customer and is identified in Schedule C.

"Educational Institution" means a public or private school district, school, charter school, college, university, or other educational agency or institution.

"Education Records" means has the meaning given in FERPA.

"Student Data" means any information in Customer Data that identifies, or is linked or reasonably linkable to, a current or former student of Customer, including Education Records and "covered information" under SOPPA. The categories Tellaro expects to process are listed in Schedule A.

"De-identified Data" means information from which all direct and indirect identifiers of students have been removed so that the information cannot reasonably be used to identify a student, and that Tellaro does not attempt to re-identify.

"Security Breach" means unauthorized acquisition of, access to, or disclosure of Student Data in Tellaro's possession or control that compromises its security, confidentiality, or integrity.

2. PURPOSE, ROLES, AND CONTROL

2.1 Purpose. Tellaro processes Student Data solely to provide the Service described in Schedule B, which protects the security of Customer's systems, accounts, and users, and as Customer otherwise directs in writing.

2.2 School Official. Customer designates Tellaro as a "school official" with a "legitimate educational interest" under 34 C.F.R. § 99.31(a)(1)(i)(B). Tellaro performs an institutional service for which Customer would otherwise use its own employees, is under Customer's direct control with respect to the use and maintenance of Education Records, and will not re-disclose Education Records except as permitted by 34 C.F.R. § 99.33 and this Addendum.

2.3 Ownership and Control. As between the parties, Student Data is Customer's property and remains under Customer's control. Customer is responsible for providing any notices to, and obtaining any consents from, students, parents, and guardians that Applicable Student Privacy Laws require for Customer's use of the Service.

2.4 Higher Education. Where Customer is a postsecondary institution, SOPPA and the K-12 provisions of Schedule C do not apply, and FERPA governs.

3. PROHIBITED USES

Tellaro will not:

- (a) sell, rent, or trade Student Data;
- (b) use Student Data for targeted advertising, or to build a profile of a student for any purpose other than providing the Service to Customer;
- (c) use Student Data for any purpose other than providing the Service, complying with law, or protecting the security of the Service;
- (d) disclose Student Data to any third party except (i) to Customer, (ii) to Sub-Processors bound by written obligations at least as protective as this Addendum, (iii) as required by law, after notice to Customer where legally permitted, or (iv) as Customer directs in writing; or
- (e) include Student Data in Threat Indicators shared under Section 7.2A of the Agreement or Section 2.5 of the DPA. Tellaro may use De-identified Data to improve its security services, and will not sell it or attempt to re-identify it.

4. SECURITY

Tellaro will maintain reasonable security procedures and practices that align with industry standards (including the NIST Cybersecurity Framework), as described in Schedule 2 of the DPA and verified by Tellaro's SOC 2 Type II report. Tellaro will limit access to Student Data to personnel and Sub-Processors who need it to provide the Service and who have received privacy and security training.

5. SECURITY BREACH

5.1 Notice. Tellaro will notify Customer of a confirmed Security Breach without unreasonable delay and in any event within seventy-two (72) hours after confirming it, which satisfies the 30-day notice period under SOPPA and the 7-day period under New York Education Law § 2-d. The notice will include, to the extent known, the date of the breach, the categories of Student Data affected, the number of students affected, and the steps Tellaro has taken, and Tellaro will supplement it as information becomes available.

5.2 Cooperation. Tellaro will reasonably cooperate with Customer's investigation and with any notifications Customer is required to make. Customer is responsible for notifying students, parents, guardians, and regulators, unless the parties agree otherwise in writing.

5.3 Cost Allocation. If a Security Breach is attributable to Tellaro's breach of this Addendum, Tellaro will reimburse Customer's reasonable, documented costs of investigating and remediating the Security Breach, including notification costs, credit monitoring, legal fees, audit costs, and fines imposed on Customer, in proportion to Tellaro's responsibility for the Security Breach. Costs attributable to Customer's acts or omissions remain with Customer. Tellaro's obligations under this Section 5.3 are Data Protection Claims subject to the super-cap in the Agreement, except to the extent an Applicable Student Privacy Law prohibits that limitation.

6. REQUESTS FROM STUDENTS, PARENTS, AND GUARDIANS

Tellaro will forward to Customer any request it receives directly from a student, parent, or guardian to review, correct, or delete Student Data, and will not respond to it except as Customer directs. Tellaro will assist Customer in responding within the time Applicable Student Privacy Laws require, to the extent the Student Data is in Tellaro's possession.

7. RETENTION AND DELETION

7.1 On Request. Tellaro will delete Student Data that Customer identifies in a written request within thirty (30) days after the request, unless the Student Data must be retained to provide the Service, in which case Tellaro will tell Customer and the parties will agree on an alternative.

7.2 At Termination. Tellaro will delete Student Data within thirty (30) days after the post-termination export period in the Agreement ends, and will certify deletion in writing on Customer's request. Student Data in backups is deleted as backups expire on Tellaro's standard schedule, not to exceed ninety (90) days, and remains protected under this Addendum until then.

7.3 Self-Hosted and Hybrid. Student Data stored in the Customer Environment or in Customer-Hosted Components is retained and deleted by Customer. This Section 7 applies only to Student Data in Tellaro's possession.

8. SUB-PROCESSORS AND PUBLIC DISCLOSURE

Tellaro's Sub-Processors are listed in Schedule 1 of the DPA, and changes follow Section 4.2 of the DPA. Customer may publish this Addendum and the Sub-Processor list on its website as SOPPA or other law requires, provided that Customer redacts pricing and Tellaro's security documentation.

9. LIABILITY, TERM, AND PRECEDENCE

9.1 Liability. This Addendum is subject to the limitations and exclusions of liability in the Agreement, including the data protection super-cap, except to the extent an Applicable Student Privacy Law prohibits a limitation.

9.2 Term. This Addendum remains in effect for as long as Tellaro holds Student Data.

9.3 State Terms. Schedule C contains state-specific terms. If Customer is subject to a state student-privacy law not addressed in Schedule C, the parties will negotiate in good faith a rider containing only the terms that law requires.

SCHEDULE A — CATEGORIES OF STUDENT DATA

Category	Examples

Directory and identity data	Name, username, email address, student ID, group and role membership
Device data	Hostnames, device identifiers, and IP addresses of student-assigned devices
Authentication and activity logs	Sign-in events, MFA events, access logs, and session data
Endpoint security telemetry	Process, file, and network events on student devices
Email security data	Metadata of reported or suspicious messages and, where needed for triage, message content
Security alerts and case data	Alerts, investigation notes, and response actions involving student accounts or devices

The Service is not designed to collect grades, health, disciplinary, special-education, or other academic records. Customer will configure data sources so that such records are not sent to the Service. Any such records that are captured incidentally are Student Data under this Addendum.

SCHEDULE B — DESCRIPTION OF THE SERVICE

Security monitoring, detection, and response for Customer's identity directory, Microsoft 365 tenant, endpoints, and other connected systems, under the Plan identified on the Order Form and described in the Service Descriptions (Exhibit E). The Service protects Customer's systems and users. It is not an instructional, assessment, or student-information system.

SCHEDULE C — STATE-SPECIFIC TERMS

C.1 Illinois (SOPPA)

- Tellaro is an "operator" acting as a school official for Customer (Section 2.2).
- Categories of covered information: Schedule A. Product functions: Schedule B.
- Breach notice: Section 5.1. Cost allocation: Section 5.3. Deletion: Section 7.
- Customer may publish this Addendum and the Sub-Processor list (Section 8).

C.2 New York (Education Law § 2-d; 8 NYCRR Part 121)

- Customer will attach its Parents' Bill of Rights for Data Privacy and Security and the supplemental information it requires. Tellaro will complete the supplemental information on request.
- Tellaro's data security and privacy plan consists of DPA Schedule 2, its SOC 2 Type II controls, and this Addendum, and aligns with the NIST Cybersecurity Framework.
- Breach notice within seven (7) calendar days is satisfied by Section 5.1.

C.3 California (Education Code § 49073.1; Business and Professions Code § 22584)

- The Service does not store pupil-generated content. Pupil records remain the property and under the control of Customer (Section 2.3). Sections 3 through 7 contain the required use, security, breach, and deletion terms.

SIGNATURE

The parties have executed this document by their authorized representatives below.

Tellaro	Customer
Legal name: H&A Security Solutions, LLC d/b/a Tellaro	Legal name: [CUSTOMER LEGAL NAME]
Signature: _____	Signature: _____
Printed name: _____	Printed name: _____
Title: _____	Title: _____
Date: _____	Date: _____