Addendum E

PARENTS' BILL OF RIGHTS - SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE:** The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by **(the "Vendor")** are limited to the purposes authorized in the contract between the Vendor and Sullivan County BOCES **(the "BOCES")** dated 7/24/2023________ **(the "Contract Date")**.

2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Vendor will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to, those outlined in applicable State and Federal laws and regulations (e.g., Family Educational Rights and Privacy Act ("FERPA"); Education Law § 2-d; 8 NYCRR § 121).

3. **CONTRACT PRACTICES:** The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be permanently de-identified or exported to the BOCES in: (choose one)

   □ The agreed upon format to BOCES (or)

   ☒ Will be destroyed by the Vendor as directed by the BOCES

4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in the FERPA, stored by the BOCES in a Vendor's product and/or service by following the BOCES's procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by BOCES in Vendor's product and/or service by following the appeal procedure in the BOCES's APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES:** Confidential Data provided to Vendor by the BOCES will be stored at **Amazon Web Service**. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework, including but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES:** The Vendor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Addendum F

VENDOR'S DATA SECURITY AND PRIVACY PLAN COMPONENTS

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	We have a dedicated Data Security Team who is responsible for implementing security measures for the protection of PII data and being compliant with required frameworks.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	We don't keep all data, we only keep what is necessary to conduct the business. Data is strongly encrypted using industry standard encryption. Additionally, we've created policies and procedures for handling PII, as well as offering training on it.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	We offer our employees and require them to pass the FERPA training as well as Security Awareness training. Subcontractors are also required to undergo training.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	We have contracts, Service Level Agreements (SLA), and Non-Disclosure Agreements (NDA). As part of our third-party relationship management, we obtain an understanding of whether our third parties will be subcontracting any of their obligations and whether our agreement terms and conditions flow through to them.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	We have a team dedicated to the prevention and safeguards of PII. In the event of a breach, we have a Data Breach Response Policy and an Incident Response and Management Policy in place.

6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Because our software is designed to enable students to continue accessing their data after graduation, the data never becomes obsolete or is transitioned. If data is required by the EA, a request in writing is needed. Data in motion and at rest (stored) is encrypted using strong industry-standard encryption.
7	Describe your secure destruction practices and how certification will be provided to the EA.	If data destruction is requested in writing by the EA or the data owner, we will follow the de-identification process to prevent our data sets from containing any PII. Destruction certificates can be provided by request. Note: We do not destroy data, we permanently deidentified it.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	The frameworks we follow aligned with EA's policies are FERPA and NIST.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Physical devices and systems within the organization are inventoried as well as software platforms and applications within the organization. We've also mapped out the organization's communication and data flows. The information can be found in our YouScience Asset Management Policy.
Function	Category	Contractor Response
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Priorities for the organization's mission, objectives, and activities have been established and communicated. Additionally, we have determined critical objectives, capabilities, and services for risk management decisions.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Priorities for the organization's mission, objectives, and activities are established and communicated, and we have identified YouScience's place in critical infrastructure and its industry sector.

	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Processes have been established to receive, analyze and respond to vulnerabilities found through a variety of scans, tests, assessments, and processes following our YouScience Risk Management Policy. Critical outcomes, capabilities, and services that the organization relies on are determined and communicated. Risks are proactively tracked and reviewed regularly.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Responsibility and accountability are determined and communicated for ensuring that the risk management strategy and program created by YouScience are resourced, implemented, assessed, and maintained.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	Contracts with suppliers, service providers and third-party partners are used to implement appropriate measures designed to meet the objectives of YouScience's Risk Management Plan.
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Identities and credentials issued by YouScience are managed, verified, revoked, and audited for authorized devices, users, and processes.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Security awareness and training are periodically provided for YouScience personnel so they possess the knowledge and skills to perform their tasks.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	The confidentiality, integrity, and availability of data-at-rest and data-in-transit are protected. Protections against data leaks have been implemented. And the confidentiality, integrity, and availability of data-in-use are also protected.
unction	Category	Contractor Response
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Response and recovery plans (e.g., incident response plan, business continuity plan, disaster recovery plan, contingency plan) have been created, shared with YouScience employees, and maintained.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Systems, devices, and software used/issued by YouScience are managed throughout their life cycle, including pre-deployment checks, preventive maintenance, and disposition.

	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Log records are generated for cybersecurity events and made available for continuous monitoring. Secure software development practices are integrated and their performance is monitored throughout the software development life cycle (SDLC). Backups of platform software are conducted, protected, maintained, and tested. Policies and procedures for these operations have been created and maintained by the YouScience Data Security Team.
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	Incident alert thresholds have been established and adverse events are analyzed to find possible attacks, compromises, mitigation, and solutions.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Physical environment, personnel activity, technology usage, software and their data, and network services are monitored by the YouScience Data Security Team to find adverse cybersecurity events.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Continuous evaluations, including reviews, audits, assessments, security tests, and exercises, are carried out to find anomalous events and identify improvements.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	The YouScience Incident Response Plan has been created and is regularly revised and maintained.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Information is shared on a need-to-know basis with internal and external stakeholders and law enforcement as required by the law and as directed by YouScience's security policies.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	An analysis could be performed by the YouScience Data Security Team to determine what has taken place during an incident and the root cause of the incident. Actions performed during an investigation will need to be recorded and the record's integrity and provenance will need to be preserved.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Risk responses will need to be identified and prioritized by the YouScience Data Security Team. Newly identified vulnerabilities will need to be mitigated or documented as accepted risks.
unction	Category	Contractor Response
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Improvements for processes and activities across all Framework Functions will need to be identified based on lessons learned and response strategies will need to be created/updated by the YouScience Data Security Team.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	In case of an incident, the YouScience incident recovery plan will be implemented. Recovery actions determined, scoped, prioritized, and performed in accordance with the plan will need to be executed. The integrity of restored assets will need to be verified, systems and services will need to be restored, and the team will also need to confirm normal operating status.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	A plan is in place to ensure that improvements for processes and activities across all Framework Functions will be identified based on lessons learned and response strategies will be created/updated by the YouScience Data Security Team.

	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	After an Incident, YouScience will need to mitigate any negative repercussions. Recovery activities and progress in restoring operational capabilities will need to be communicated to all pertaining parties.

Addendum G

SUPPLEMENTAL TERMS

These Supplemental Terms to Sullivan BOCES Software License Vendor Agreement ("**Supplemental Terms**") are entered into effective as of 7/21/2023 ("**Supplemental Terms Effective Date**") by and between Sullivan County BOCES ("**BOCES**") and YouScience, LLC ("**Vendor**").

WHEREAS, the Parties wish to enter into this Supplemental Terms to ensure the Sullivan BOCES Software License Vendor Agreement entered into by and between BOCES and Vendor of even date herewith (the "**Agreement**") conforms to the requirements of the privacy laws referred to therein and the nature of the Services provided by Vendor to BOCES pursuant to one or more purchase orders (the "**Service Agreement**").

WHEREAS, the Parties desire to incorporate this Supplemental Terms into the Agreement to describe the Parties' duties and responsibilities to protect data transmitted to Vendor from BOCES in order to facilitate the provision of the services outlined in Addendum A – Description of Services (the "**Services**").

NOW THEREFORE, for good and valuable consideration, the Parties hereby agree to the following changes to the Agreement:

1. **Capitalized Terms.** Capitalized terms used but not defined in this Supplemental Terms shall have the meanings given to them in the Agreement except as modified herein.

2. **Scope.** The Parties hereby acknowledge and agree that all purchase orders submitted by BOCES to Vendor under the Service Agreement are subject to the terms of the Agreement and this Supplemental Terms, as applicable.

3. **Interpretation.** In the event of any conflict between the terms of this Supplemental Terms and the terms of the Agreement, the terms of this Supplemental Terms shall control. The Parties further agree that any changes to the Agreement necessary to conform the Agreement to the terms of this Supplemental Terms are hereby deemed made.

4. **Confidential Information to Be Provided.** The Parties acknowledge and agree that, with respect to the data to be provided in connection with the Services, the data provided by BOCES constitutes Confidential Data and the data provided or generated by a student constitutes Student Generated Content.

5. **Scope of Confidential Data.** In addition to, and not in lieu of, any additional exclusions from the types of data, materials, content, and other information that constitute Confidential Data under the Agreement, the Parties agree that neither Confidential Data nor Student Data include any Student Generated Content.

6. **Ownership of Student Generated Content.** As between BOCES and Vendor, all Student Generated Content is and will continue to be the property of the student, or, where applicable, the student's parent or legal guardian, who provided or generated such Student Generated Content.

7. **Access to Confidential Data and Student Generated Content.**

    a. **General.** Subject to Vendor's continued obligations under the Service Agreement, the Agreement, and this Supplemental Terms, BOCES acknowledges and agrees that each student, or, where applicable, such student's parent or legal guardian, will have a continuous right through Vendor's standard features and functionalities available through the Services to access such student's:

        1. Confidential Data during the term of the Service Agreement; and

        2. Student Generated Content for the period of the license granted by Vendor to such student, or, where applicable, to such student's parent or legal guardian, as described in Description of Services, attached to the Agreement as Addendum A.

    b. **Parent Access.** Vendor will provide reasonable assistance to BOCES to enable BOCES to provide parental access and the ability to correct erroneous information by making Vendor's standard features and functionalities available to BOCES through the Services that enable BOCES to engage in or facilitate such activities.

8. **Separate Account.** For each student, Vendor will maintain separate accounts – one for any Student Generated Content, and one for Confidential Data stored or maintained by Vendor.

9. **Annual Notification of Rights.** In addition to, and not in lieu of BOCES's duties under the Agreement, BOCES shall also provide the means by which BOCES, eligible students, and, where applicable, parents or legal guardians may consent to the disclosure of Student Generated Content to a third party.

10. **Authorized Use.** BOCES acknowledges and agrees that Vendor is authorized to disclose data as necessary to provide the Services, and in doing so, Vendor acknowledges that it shall not make any re-disclosure of any Confidential Data or any portion thereof without the express written consent of BOCES, and shall not make any redisclosure of any Student Generated Content without the express written consent of the student or the applicable parent or legal guardian.

11. **Disposition of Confidential Data.** BOCES may instruct Vendor to permanently de-identify Confidential Data through the features and functionalities available to BOCES through the Services, or via e-mail.

12. **Advertising Limitations.** In addition to, and not in lieu of, any exceptions to the use of Confidential Data for advertising purposes set forth in the Agreement, BOCES acknowledges and agrees that Vendor may use the Confidential Data to provide the Services to students and as otherwise detailed in Addendum A.

13. **Data Breach.** In the event that Confidential Data or Student Generated Content in Vendor's possession or under its reasonable control is accessed or obtained by an unauthorized individual, Vendor shall notify BOCES within a reasonable amount of time after which the Vendor learns of the incident (not to exceed forty-eight (48) hours).

14. **Integration Clause.** Any modification or waiver under this Supplemental Terms will be effective only if it is in writing and signed by the Parties to be bound. This Supplemental Terms, when fully executed by authorized representatives of the Parties, shall form part of, and be subject to the terms set forth in, the Agreement as amended. Except as amended and modified by this Supplemental Terms, the terms and provisions of the Agreement remain unchanged and in full force and effect.

IN WITNESS WHEREOF, the Parties have caused this Supplemental Terms to be executed by their duly authorized representatives as of the Supplemental Terms Effective Date.

SULLIVAN COUNTY BOCES	**YOUSCIENCE, LLC**
Signature	Signature
	J. Philip Hardin
Printed Name	Printed Name
	Chief Financial Officer
Title	Title
9/19/23	July 24, 2023
Date	Date

AMENDMENT

THIS AMENDMENT entered into on July 24, 2024 amends the Software License Vendor Agreement dated July 24, 2023 entered into by and between the Sullivan County BOCES ("BOCES") and YouScience, LLC ("Vendor") ("Agreement").

WHEREAS, the Agreement expires on July 24, 2024; and

WHEREAS, BOCES and Vendor desire to extend the term of the Agreement as reflected herein.

NOW THEREFORE, for valuable consideration the Parties hereto amend the Agreement as follows:

1. **Term.** The Term of the Agreement is hereby extended for one (1) year, such that the Term shall expire on July 24, 2025.

2. **Conflict.** In the event of a conflict between the terms of this Amendment and the terms of the Agreement, the terms of this Amendment shall control. All of the defined terms in the Agreement shall have the same definitions in this Amendment, unless otherwise defined herein.

3. Except as expressly set forth in this Amendment, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Parties hereto have executed this Amendment as of the date first set forth above.

SULLIVAN COUNTY BOCES	**VENDOR**
______________________	______________________
Signature	Signature
RM DUFOUR	J. Philip Hardin
Name	Name