

DATA PRIVACY AGREEMENT

Shenendehowa Central School District

and

YouScience, LLC

This Data Privacy Agreement ("DPA") is by and between the Shenendehowa Central School District ("EA"), an Educational Agency, and **YouScience, LLC** ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.



8. **NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated **November 11th** ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New



York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST CyberSecurity Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII



shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Except as necessary to provide the services outlined in Exhibit D – Description of Services, Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access. The foregoing requirement shall not apply to any Subcontractors whose services are limited to hosted data storage or technology infrastructure services.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its subcontractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.



12. Breach.

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.
- (b) Notifications required under this paragraph must be provided to the EA at the following address:

Rebecca Carman
Shenendehowa District Privacy Officer
5 Chelsea Place
Clifton Park, NY 12065
carmrebe@shenschools.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's legally required notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.



15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.



2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

3. Exhibits.

Exhibits A – Bill of Rights, B – Supplemental Information, C – Data Security and Privacy Plan, D – Description of Services, and E – Addendum attached hereto are hereby incorporated as though set forth herein in their entirety.

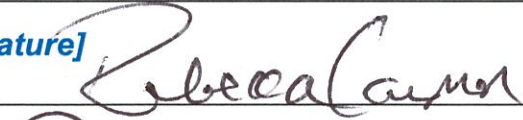
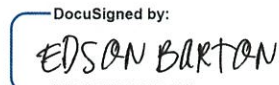


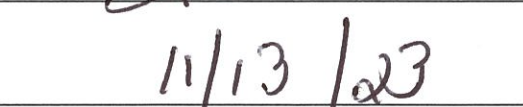
EDUCATIONAL AGENCY	CONTRACTOR: YouScience, LLC
BY: [Signature] 	BY: <small>DocuSigned by:</small>  <small>7BD5C7753A4C435...</small>
[Printed Name] 	Edson Barton
[Title] 	CEO
Date: 	11/1/2023

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, place of birth, social security number, biometric record & mother's maiden name, which when linked to or combined with other information that, alone or in combination, is linked or linkable to a specific student and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or any information requested by a person if the educational agency or institution reasonably believes that person knows the identity of the student to whom the education record relate
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the Shenendehowa Central School District, Director of Policy & Community Development/Data Protection Officer, 5 Chelsea Place, Clifton Park, NY 12065. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR: YOUSCIENCE, LLC

[Signature]

DocuSigned by:

EDSON BARTON

7BD5C7753A4C435...

[Printed Name]	Edson Barton
[Title]	CEO
Date:	11/1/2023

EXHIBIT B

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	YouScience, LLC
Description of the purpose(s) for which Contractor will receive/access PII	<p>YouScience is a career connected learning system that gives students the opportunity for personal self-discovery, career exploration, skills demonstration, work-based learning experiences, connections to post-secondary institutions, and connections to employers. The specific services provided are subject to the purchase order with the School.</p> <p>YouScience provides the Student with one or more of the following services pursuant to the Terms of Use available at https://www.youscience.com/terms-of-use/, each of which either constitutes or generates Student Generated Content:</p> <ul style="list-style-type: none"> • Separate student account to access Student Generated Content for up to 10-years. The length of access depends on the specific service (e.g. Summit and certification results are 10 years, Snapshot results are 3 years). • Performance measures of aptitudes • Life-long credentials of value for communication to employers and post-secondary institutions • Interest surveys • Personality, learning style, and other self-awareness tools • Interpersonal survey • Personalized feedback • Career discovery • Resume generation and self-advocacy language • Academic planning • Work-based learning administration • Education Connections (post-secondary education information and opportunities) <ul style="list-style-type: none"> ○ Recommended majors based upon interests, aptitudes, certifications, and other user input ○ Display logos and content from contextually relevant post-secondary education institutions for the purpose of aiding students

	<p>in understanding a broad range of available educational opportunities</p> <ul style="list-style-type: none"> ○ When available, the opportunity to connect directly with post-secondary education providers • Employer Connections (local internship, work study, and employment information and opportunities) <ul style="list-style-type: none"> ○ Recommended internship, work study, and employment opportunities based upon interests, aptitudes, certifications, and other user input ○ Display contextually relevant employer logos or other employer content for the purpose of aiding students in understanding a broad range of available employment opportunities ○ When available, the opportunity to connect directly with local employers <p>YouScience provides the faculty of School with one or more the following services based on the purchase order with the School:</p> <ul style="list-style-type: none"> • Ability to experience the aptitude assessment and career guidance personally • Invitation management • View student results on an individual basis • Track student progress individually and across groups • Administrative reporting • Academic advising reporting • Academic planning • Work-based learning administration • Exam proctoring, which may include remote proctoring <p>YouScience provides aggregated, de-identified analytics for education recruitment, economic development, and workforce purposes.</p>
Type of PII that Contractor will receive/access	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input type="checkbox"/> APPR Data</p>
Contract Term	<p>Contract Start Date <u>11/1/2023</u></p> <p>Contract End Date <u>10/31/2026</u></p>

Subcontractor Written Agreement Requirement	<p>Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option)</p> <p><input type="checkbox"/> Contractor will not utilize subcontractors.</p> <p><input checked="" type="checkbox"/> Contractor will utilize subcontractors.</p>
Data Transition and Secure Destruction	<p>Upon expiration or termination of the Contract, Contractor shall:</p> <ul style="list-style-type: none"> • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	<p>Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.</p>
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p>
Encryption	<p>Data will be encrypted while in motion and at rest.</p>

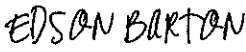
CONTRACTOR: YOUSCIENCE, LLC	
[Signature]	<div>DocuSigned by:  <small>7BD5C7753A4C435...</small></div>
[Printed Name]	Edson Barton
[Title]	CEO
Date:	11/1/2023

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

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 just 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 and 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.

ATTACHMENT 1(A) – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

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 flow. 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, risk analyses, 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.
	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.

PROTECT (PR)	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.

Function	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 periodically 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 and alerts 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.
	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.

RESPOND (RS)	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 are mitigated or documented as accepted risks.

Function	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 be restored, and the team will also 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 mitigate any negative repercussions. Recovery activities and progress in restoring operational capabilities will be communicated to all pertaining parties.

EXHIBIT D – DESCRIPTION OF SERVICES

YouScience is a career connected learning system that gives students the opportunity for personal self-discovery, career exploration, skills demonstration, work-based learning experiences, connections to post-secondary institutions, and connections to employers. The specific services provided are subject to the purchase order with the School.

YouScience provides the Student with one or more of the following services pursuant to the Terms of Use available at <https://www.youscience.com/terms-of-use/>, each of which either constitutes or generates Student Generated Content:

- Separate student account to access Student Generated Content for up to 10-years. The length of access depends on the specific service (e.g. Summit and certification results are 10 years, Snapshot results are 3 years).
- Performance measures of aptitudes
- Life-long credentials of value for communication to employers and post-secondary institutions
- Interest surveys
- Personality, learning style, and other self-awareness tools
- Interpersonal survey
- Personalized feedback
- Career discovery
- Resume generation and self-advocacy language
- Academic planning
- Work-based learning administration
- Education Connections (post-secondary education information and opportunities)
 - Recommended majors based upon interests, aptitudes, certifications, and other user input
 - Display logos and content from contextually relevant post-secondary education institutions for the purpose of aiding students in understanding a broad range of available educational opportunities
 - When available, the opportunity to connect directly with post-secondary education providers
- Employer Connections (local internship, work study, and employment information and opportunities)
 - Recommended internship, work study, and employment opportunities based upon interests, aptitudes, certifications, and other user input
 - Display contextually relevant employer logos or other employer content for the purpose of aiding students in understanding a broad range of available employment opportunities
 - When available, the opportunity to connect directly with local employers

YouScience provides the faculty of School with one or more the following services based on the purchase order with the School:

- Ability to experience the aptitude assessment and career guidance personally
- Invitation management
- View student results on an individual basis
- Track student progress individually and across groups
- Administrative reporting
- Academic advising reporting
- Academic planning
- Work-based learning administration
- Exam proctoring, which may include remote proctoring

YouScience provides aggregated, de-identified analytics for education recruitment, economic development, and workforce purposes.

EXHIBIT E – ADDENDUM TO DATA PRIVACY AGREEMENT

This Addendum to Data Privacy Agreement (this “**Addendum**”) is entered into effective as of 11/1/2023 (“**Addendum Effective Date**”) by and between Shenendehowa Central School District (“**EA**”) and YouScience, LLC (“**Contractor**”).

WHEREAS, the Parties wish to enter into this Addendum to ensure the Data Privacy Agreement entered into by and between EA and Contractor of even date herewith (the “**DPA**”) conforms to the requirements of the privacy laws referred to therein and the nature of the Services provided by Contractor to EA pursuant to one or more purchase orders (the “**Service Agreement**”).

WHEREAS, the Parties desire to incorporate this Addendum into the DPA to describe the Parties’ duties and responsibilities to protect data transmitted to Contractor from EA in order to facilitate the provision of the services outlined in Exhibit D – Description of Services (the “**Services**”).

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

1. **Capitalized Terms.** Capitalized terms used but not defined in this Addendum shall have the meanings given to them in the DPA except as modified herein.
2. **Scope.** The Parties hereby acknowledge and agree that all purchase orders submitted by EA to Contractor under the Service Agreement are subject to the terms of the DPA and this Addendum, as applicable.
3. **Interpretation.** In the event of any conflict between the terms of this Addendum and the terms of the DPA, the terms of this Addendum shall control. The Parties further agree that any changes to the DPA necessary to conform the DPA to the terms of this Addendum 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 EA constitutes Student Data or PII and the data provided or generated by a student constitutes Student Generated Content.
5. **Scope of Student Data/PII.** In addition to, and not in lieu of, any additional exclusions from the types of data, materials, content, and other information that constitute Student Data or PII under the DPA, the Parties agree that neither Student Data nor PII include any Student Generated Content.
6. **Ownership of Student Generated Content.** As between EA and Contractor, 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 Student Data/PII and Student Generated Content.** Subject to Contractor’s continued obligations under the Service Agreement, the DPA, and this Addendum, EA acknowledges and agrees that each student, or, where applicable, such student’s parent or legal guardian, will have a continuous right through Contractor’s standard features and functionalities available through the Services to access such student’s:
 1. Student Data/PII during the term of the Service Agreement; and
 2. Student Generated Content for the period of the license granted by Contractor to such student, or, where applicable, to such student’s parent or legal guardian, as described in Description of Services, attached to the DPA as Exhibit D.
8. **Separate Account.** For each student, Contractor will maintain separate accounts – one for any Student Generated Content, and one for Student Data/PII stored or maintained by Contractor.

9. **Annual Notification of Rights.** In addition to, and not in lieu of EA's duties under the DPA, EA shall also provide the means by which EA, 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.** EA acknowledges and agrees that Contractor is authorized to disclose data as necessary to provide the Services, and in doing so, Contractor acknowledges that it shall not make any re-disclosure of any Student Data/PII or any portion thereof without the express written consent of EA, 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 Student Data/PII.** EA may instruct Contractor to permanently de-identify Student Data or PII through the features and functionalities available to EA through the Services, or via e-mail.
12. **Advertising Limitations.** In addition to, and not in lieu of, any exceptions to the use of Student Data or PII for advertising purposes set forth in the DPA, EA acknowledges and agrees that Contractor may use the Student Data or PII to provide the Services to students and as otherwise detailed in Exhibit D, including upon request of the student, connecting students with potential post-secondary education opportunities and potential employment opportunities. Contractor may receive compensation from post-secondary educational institutions and/or employers for its provision of such connection services.
13. **Data Breach.** In the event that Student Data/PII or Student Generated Content in Contractor's possession or under its reasonable control is accessed or obtained by an unauthorized individual, Contractor shall notify EA within a reasonable amount of time after which the Contractor learns of the incident (not to exceed forty-eight (48) hours).
14. **Integration Clause.** Any modification or waiver under this Addendum will be effective only if it is in writing and signed by the Parties to be bound. This Addendum, when fully executed by authorized representatives of the Parties, shall form part of, and be subject to the terms set forth in, the DPA as amended. Except as amended and modified by this Addendum, the terms and provisions of the DPA remain unchanged and in full force and effect.

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

Shenendehowa Central School District

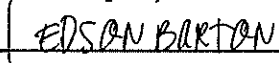
Signature

Printed Name

Title

Date

YOUSCIENCE, LLC

DocuSigned by:

7BD5C7753A4C435...
Signature

Edson Barton
Printed Name

Chief Executive Officer
Title

November 1, 2023
Date