HERKIMER CENTRAL SCHOOL DISTRICT
DATA PRIVACY AGREEMENT

Herkimer Central School District

and

Wilson Language Training

This Data Privacy Agreement ("DPA") is by and between the [Herkimer Central School District] ("EA"), an Educational Agency, and [Wilson Language Training] ("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 in an unencrypted format 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 and who have unencrypted access to Student Data.

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 [5/06/24] or an accepted quote and purchase order, and Contractor will provide those products and services pursuant to the Wilson Language Training Corporation's Digital Products Terms of Service, available at https://www.wilsonlanguage.com/digital-products-terms-of-service/ ("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 Cyber Security 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 a summary 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. Contractor may provide the EA with a summary of 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 confidentiality obligations consistent with, and no less protective than 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 their confidentiality and data-security commitments to Contractor, 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 their confidentiality and data-security commitments to Contractor. 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) 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 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.

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors 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, and following written request by the EA, 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) Upon written request, 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 reasonable removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party except as permitted under applicable law.

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:

[Name: Richard C. Mathy Jr.

Title: Data Privacy Officer

Address: 801 West German Street

City, State, Zip: Herkimer NY, 13350

Email: RMathy@Herkimercsd.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 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 Band append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit Bon 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.

EDUCATIONAL AGENCY	**CONTRACTOR**
BY: Richard C Mathy Jr.	BY: SIGNED WITH IRONCLAD Josh Minty f52b2c48-bde0-498a-8c...
Richard C. Mathy Jr.	***Josh Minty***
Data Privacy Officer	**General Counsel**
Date:	Date: 5/6/2024

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, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

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 EA at: [rmathy@herkimercsd.org). (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	
[Signature]	Josh Minty
[Printed Name]	Josh Minty
[Title]	General Counsel
Date:	5/6/2024

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	Wilson Language Training Corporation
Description of the purpose(s) for which Contractor will receive/access PII	To provide Wilson's Digital Products (such as FUN HUB®) to the District.
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII D APPR Data
Contract Term	Contract Start Date 5/6/2024 Contract End Date 6/30/2025 or until EA ceases to use Digital Services
Subcontractor Written Agreement Requirement	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) □ Contractor will not utilize subcontractors. ☑ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • 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	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.

Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☑ Using a cloud or infrastructure owned and hosted by a third party. □ Using Contractor owned and hosted solution □ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: We have implemented the following administrative, operational, and technical safeguards in connection with the provision our Digital Products: a) **User Access**. Use of an account and a password is required to access our Digital Products. We do not offer users, including students, any way to login to our Digital Products through social media tools. b) **Employee Access.** Access to customer data is limited (through user/password credentials and two factor authentication) to those employees who require it to perform their job functions. Our employees with access to customer data will receive training on data privacy (including on FERPA and New York Education Law 2d) prior to receiving access and on an annual basis thereafter. All employees must sign a confidentiality agreement before they join the company, and background checks are conducted as part of the onboarding process. We conduct phishing and social-engineering awareness testing and education for our employees. c) **Storage and processing.** Student data is stored in the United States. We maintain strict administrative, technical, and physical procedures to protect customer data stored in our servers, which are located across Tier 1 data centers that are logically and physically separated locations. Our hosting provider implements security measures in accordance with industry standards. d) **Encryption.** We use industry-standard Secure Socket Layer (SSL) encryption technology to safeguard the account registration process and sign-up information. Other security safeguards include but are not limited to data encryption, firewalls, and physical access controls to buildings and files. Data is encrypted during transmission and at rest. e) **Device Controls**. We encrypt all of our employee laptops, and those devices are centrally managed and covered by anti-virus protections which are updated periodically. Laptops are password protected.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	Josh Minty
[Printed Name]	Josh Minty
[Title]	General Counsel
Date:	5/6/2024

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

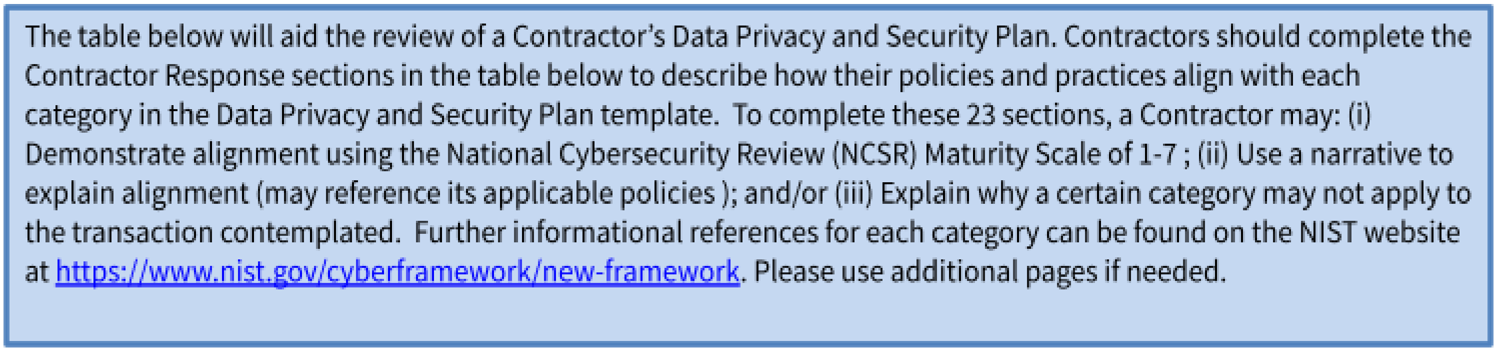
The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law§ 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a 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.	Contractor implements data security and privacy contract requirements according to Contractor Digital Products Privacy Statement: https://www.wilsonlanguage.com/digital-products-privacy-statement/ and the IT Security Standards: https://www.wilsonlanguage.com/information-technology-security-standards/ For questions regarding these two policies, please contact legal@wilsonlangauge.com
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	We have implemented the following administrative, operational, and technical safeguards in connection with the provision our Digital Products: a) **User Access**. Use of an account and a password is required to access our Digital Products. We do not offer Users, including Students, any way to login to our Digital Products through social media tools. b) **Employee Access.** Access to customer data is limited (through user/password credentials and two factor authentication) to those employees who require it to perform their job functions. Our employees with access to customer data will receive training on data privacy (including on FERPA and New York Education Law 2d) prior to receiving access and on an annual basis thereafter. All employees must sign a confidentiality agreement before they join the company, and background checks are conducted as part of the onboarding process. We conduct phishing and social-engineering awareness testing and education for our employees. c) **Storage and processing.** Student Data is stored in the United States. We maintain strict administrative, technical, and physical procedures to protect customer data stored in

		our servers, which are located across Tier 1 data centers that are logically and physically separated locations. Our hosting provider implements security measures in accordance with industry standards. d) **Encryption.** We use industry-standard Secure Socket Layer (SSL) encryption technology to safeguard the account registration process and sign-up information. Other security safeguards include but are not limited to data encryption, firewalls, and physical access controls to building and files. Data is encrypted during transmission and at rest. e) **Device Controls**. We encrypt all of our employee laptops, and those devices are centrally managed and covered by
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.	Contractor employees with access to EA's data will receive training on data privacy prior to receiving access and on an annual basis thereafter. Employees and subcontractors are bound by applicable laws and are subject to written agreements with provisions that are consistent with the data-protection obligations imposed on Contractor in our standard data-privacy agreements with customers.
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.	All employees of Contractor must sign a confidentiality agreement before they join the company, and background checks are conducted as part of the onboarding process. We may share customer data with service providers who support our provision of the Digital Products by offering us hosting services, information technology and support (e.g., video hosting), IT security, analytics, and technologies that enhance and personalize a User's experience with the Digital Products. We evaluate the privacy and security controls of those service providers before we agree to use their services. These service providers are bound by applicable laws and contractual obligations of confidentiality that are consistent with the data-protection obligations imposed on Contractor in our standard data-privacy agreements with customers.

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.	If there is any disclosure or access to any personally identifiable student data by an unauthorized party that compromises the security, confidentiality, or integrity of the student data, we will promptly notify the affected EA consistent with applicable laws, and we will use reasonable efforts to cooperate with their investigation of the incident.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon the written request, Contractor will remove EA data from our production servers when we will no longer be providing access to the digital products to the EA. We reserve the right, in our sole discretion, to remove EA data for a particular customer from our production servers following a reasonable period of time after our relationship with a EA has ended, as demonstrated by the end of contract term or EA lack of activity within the digital products. Student data is removed from backups in accordance with our data retention standards.
7	Describe your secure destruction practices and how certification will be provided to the EA.	If requested, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor data security and privacy practices align with is consistent with applicable laws and regulations, including, without limitation, the Federal Family Educational Rights and Privacy Act (FERPA), New York Education Law 2-D (including its implementing regulations), and the Children's Online Privacy Protection Act (COPPA).and with the NIST Cyber Security Framework.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF vl.1using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 - 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.	Wilson Language maintains adequate procedures and documentation surrounding Asset Management. While Wilson Language does maintain a list of vendors, the list is not formalized and there are no corresponding data maps or data flows.
	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.	Wilson identifies and assesses reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing Sensitive Information as defined by Wilson's Information Sensitivity Policy and take all necessary steps to safeguard such information, including, but not limited to: (i) providing ongoing employee (including temporary and contract employee) training; (ii) ensuring employee compliance with policies and procedures; and (iii) implementing a means for detecting and preventing security system failures.
	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.	Wilson has adopted a Comprehensive Data Security Plan in an effort to ensure the security and confidentiality of Sensitive Information as defined by WLT's Information Sensitivity Policy. Wilson conducts an information security risk assessment at least annually to take affirmative steps to correct any identified deficiencies. These assessments shall be performed by a qualified third party vendor
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Wilson performs a timely review of vulnerability information received from reputable sources and performs a proper analysis to confirm applicability of identified vulnerabilities in comparison to system inventory.

	Risk Management Strategy (ID.RM): The organization’s priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Wilson lacks a formalized Risk Management Program, but is currently working with a security consultant to actively create and adopt such a program.
	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.	As per Wilson's Comprehensive Data Security Plan, access to data is provided on an as-needed basis. Third Party Vendors and Partners who access any sensitive information must take the necessary steps to protect this data and to comply with all applicable data privacy and protection laws and regulations. All of Wilson’s third party vendors and business associates are required to implement, test, and continually monitor administrative, physical, and technical controls to protect WLT’s Sensitive Information, at least to the same degree as WLT protects such information according to Wilson’s cyber security policies.
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.	As per Wilson’s Access Control Policy: Users will be granted the minimum access required to perform their specific tasks. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities, and separation of duties. The level of minimum access requires the recommendation of the user’s manager, and the evaluation of the information system owner. The information system owner will have final determination as to the level of a user’s access for their system. Additionally: All Wilson user accounts must be unique, and traceable to the assigned user. Wilson will take appropriate measures to protect the privacy of user information associated with user accounts. The use of group accounts and group passwords is not allowed, unless specifically approved by Wilson’s CIO.
	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.	Wilson provides annual training related to cybersecurity and privacy (including Ed Law 2-d), and has a security and awareness program and is in the process of alignment with formalized documentation.
	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.	Wilson Language adequately encrypts data at rest and in transit. Wilson maintains adequate asset management tracking and is in process of formalized documentation. Wilson Language backs up data adequately. Wilson maintains IDS and IPS tools. Wilson maintains separate development and testing environments from their production environment.
	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.	Wilson configures systems on a system baseline configuration. Wilson maintains an adequate SDLC policy. Wilson maintains a Change Management Program. Wilson maintains adequate backup procedures. Wilson maintains adequate controls and documentation surrounding Physical Security. Wilson performs background checks on employees as part of the hiring process.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Wilson only allows authorized personnel to maintain and repair assets, and is currently working to document in policy.

	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.	Wilson maintains adequate logs. Wilson requires removable media to be protected but does not have formalized controls. Wilson implements the principle of least privilege to users. Wilson adequately protects communications and control networks using network segmentation and firewalls. Wilson backs up data adequately, however, there is no formal monitoring of capacity.
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	Wilson Language maintains a network diagram but lacks a data map. Wilson adequately reviews logging and alerting and is currently documenting formal procedure.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Wilson maintains adequate practices to monitor the network and detect potential cybersecurity events. Wilson Language requires badges to enter premises and guests to sign a visitor log. Wilson has adequate measures in place to detect malicious code from systems. Wilson monitors any third parties that are performing maintenance, however, there is no formal Third Party Risk Management Program. Wilson reviews and manages alerts from detection systems.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Wilson Language maintains a Security Breach Policy. Wilson reviews and manages alerts from detection systems.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Wilson maintains a Security Breach Policy.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Wilson maintains a Security Breach Policy.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Wilson reviews and manages alerts from detection systems. Wilson maintains a Security Breach Policy.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Wilson maintains a Security Breach Policy.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Wilson maintains a Security Breach Policy.
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.	Wilson is in the process of formalizing Business Continuity and Disaster Recovery Plan.
	Improvements (RC.IM): Recovery planning and processes are improved by	Wilson is in the process of formalizing Business Continuity and Disaster Recovery Plan.

🟩	incorporating lessons learned into future activities.	
	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).	Wilson is in the process of formalizing Business Continuity and Disaster Recovery Plan.

WLT New York Data Privacy and Security Plan for Digital Products

Last Updated: July 15, 2023

Purpose.
Wilson Language Training Corporation ("WLT," "we," "us," or "our") understands that privacy is incredibly important. The purpose of this *Data Privacy and Security Plan* (the "Plan") is to inform our New York customers, users, and parents of users of our Digital Products regarding our current practices for protecting the security and privacy of student data and educator data in compliance with applicable laws, including New York Education Law 2-D and its implementing regulations.

Scope.
This Plan applies to our provision of Digital Products to educators and administrators ("Educators"), to schools or school districts who purchase our Digital Products on behalf of their Educators ("Customer"), and to the students whose information we may receive from Educators, who are typically students in K-12 or beyond ("Students").
As used in this Plan:
"Digital Products" refers, collectively and individually, to FUN HUB, Virtual Implementation Support (VIS), and/or Wilson Academy.
"Educator Data" refers to information about an Educator that, either alone or in combination with other reasonably available information, can be used to identify the Educator.
"Student Data" refers to any personally identifiable information of a Student, as that term is defined under the Family Educational Rights and Privacy Act (FERPA).
"User" refers to users of our Digital Products.

1. *Data Usage in Compliance with Laws.*

Our use of Student Data is consistent with applicable laws and regulations, including, without limitation, the Federal Family Educational Rights and Privacy Act (FERPA), New York Education Law 2-D (including its implementing regulations), and the Children's Online Privacy Protection Act (COPPA). All Student Data is handled securely, as described in Section 2 below. We do not obtain any ownership interest in Student Data.

How we use Student Data

We use Student Data for the following purposes:

- to provide our Digital Products,
- to provide related reports and services to the Customer
- for customer support, and
- to comply with applicable laws.

How we use Educator Data

We use Educator Data to register and maintain Educator's account, to offer Educators the services, and to support our interactions with Educators and Customers, and to provide Educators with information concerning our programs and services, newsletters, updates, and related materials.

How We Use De-Identified Data:

We may de-identify and/or aggregate personally identifiable information, including Student Data or Educator Data, to use and share in a manner that complies with applicable laws, for our permitted business purposes, including for customer service purposes, for research and development, and to understand how our products are being used.

2. *Safeguards.*

We have implemented the following administrative, operational, and technical safeguards in connection with the provision our Digital Products:

a) **User Access**. Use of an account and a password is required to access our Digital Products. We do not offer Users, including Students, any way to login to our Digital Products through social media tools.

b) **Employee Access.** Access to Customer Data is limited (through user/password credentials and two factor authentication) to those employees who require it to perform their job functions. Our employees with access to Customer Data will receive training on data privacy (including on FERPA and New York Education Law 2d) prior to receiving access and on an annual basis thereafter. All employees must sign a confidentiality agreement before they join the company, and background checks are conducted as part of the onboarding process. We conduct phishing and social-engineering awareness testing and education for our employees.

c) **Storage and processing.** Student Data is stored in the United States. We maintain strict administrative, technical, and physical procedures to protect Customer Data stored in our servers, which are located across Tier 1 data centers that are logically and physically separated locations. Our hosting provider implements security measures in accordance with industry standards.

d) **Encryption.** We use industry-standard Secure Socket Layer (SSL) encryption technology to safeguard the account registration process and sign-up information. Other security safeguards include but are not limited to data encryption, firewalls, and physical access controls to building and files. Data is encrypted during transmission and at rest.

e) **Device Controls**. We encrypt all of our employee laptops, and those devices are centrally managed and covered by anti-virus protections which are updated periodically. Laptops are password protected.

3. **Compliance with Parents Bill of Rights.**
In connection with providing the Digital Products, Wilson hereby agrees to comply with the requirements imposed on vendors under the *Education Law 2-D Bill of Rights for Data Privacy and Security,* available at https://www.nysed.gov/sites/default/files/programs/data-privacy-security/parents-bill-of-rights_2.pdf.

4. **Employee Access.**
Access to Customer Data is limited (through user/password credentials and two factor authentication) to those employees who require it to perform their job functions. Our employees with access to Customer Data will receive training on data privacy (including on FERPA and New York Education Law 2d) prior to receiving access and on an annual basis thereafter. All employees must sign a confidentiality agreement before they join the company, and background checks are conducted as part of the onboarding process. We conduct phishing and social-engineering awareness testing and education for our employees.

5. **Subcontractors.**
We may share Customer Data with service providers who support our provision of the Digital Products by offering us hosting services, information technology and support (*e.g.*, video hosting), IT security, analytics, and technologies that enhance and personalize a User's experience with the Digital Products. We evaluate the privacy and security controls of those service providers before we agree to use their services. These service providers are bound by applicable laws and contractual obligations of confidentiality and privacy to maintain Customer Data in a secure and confidential manner.

6. Unauthorized disclosure.
If there is any disclosure or access to any personally identifiable Student Data by an unauthorized party that compromises the security, confidentiality, or integrity of the Student Data, we will promptly notify the affected Customer(s) consistent with applicable laws, and we will use reasonable efforts to cooperate with their investigation of the incident.

7. **Data Retention and Destruction.**
Upon the written request of a Customer, we will remove Customer Data from our production servers when we will no longer be providing access to the Digital Products to the Customer. We reserve the right, in our sole discretion, to remove Customer Data for a particular customer from our production servers following a reasonable period of time after our relationship with a Customer has ended, as demonstrated by the end of contract term or Customer's lack of activity within the Digital Products. Student Data is removed from backups in accordance with our data retention standards.

Electronic Record of Contracts

This document was generated as a record of certain contracts created, accepted and stored electronically.

Summary of Contracts

This document contains the following contracts.

Title	ID
Customer Contract (Herkimer Central School District and Wilson Language Training)	5bd7d296-37e4-492b-a608-08862349cd93

Contract signed by:

Josh Minty

Signer ID:	f52b2c48-bde0-496a-8c49-2f8921793517
Email:	jminty@wilsonlanguage.com

Date / Time:	May 14, 2024 at 10:08 AM EDT
IP Address:	128.92.38.130
User Agent:	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36