

Attachment C

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and NTC Language Services (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the Board of Cooperative Educational Services, First Supervisory District of Suffolk County ("ESBOCES") and Contractor, including any Agreement to Terms attached thereto, to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that ESBOCES' and/or participating school districts' Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to personally identifiable: student data, student demographics, scheduling, attendance, grades, health and discipline tracking. Protected Data also includes all other data reasonably considered to be sensitive or confidential data by ESBOCES and/or participating school districts that ESBOCES and/or the participating school district has identified to Contractor in writing as sensitive or confidential data of ESBOCES and/or the participating school district. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of ESBOCES and/or participating school districts as that term is defined in § 99.3 of FERPA,

-AND-

Personally identifiable information from the records of ESBOCES and/or participating school districts 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with ESBOCES' policy(ies) on data security and privacy provided to Contractor in advance of executing this Agreement. Contractor shall promptly reimburse ESBOCES and/or participating school districts for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall delete all of ESBOCES' and/or participating school districts' Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of ESBOCES' and/or participating school districts' Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;
6. Specifies whether Protected Data will be returned to ESBOCES and/or participating school districts, transitioned to a successor contractor, at ESBOCES' and/or participating school districts' option, or direction, deleted or destroyed by the Contractor when the contract and/or the Agreement to Terms is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of ESBOCES; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
 - a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or
 - b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, ESBOCES or the institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of ESBOCES' or participating school district's Parents' Bill of Rights.

<CONTRACTOR>

BY:  _____

DATED: 04/23/24 _____



NTC Language Services Data Security Plan

Educational Standards and Practices: NTC Language Services and its subcontractors are dedicated to aligning their services with the specific educational standards and practices outlined by various government agencies. This commitment involves using terminology and language that is appropriate for the educational context and adapting materials to ensure they are culturally relevant and accessible to all students.

A critical aspect of our service provision includes the rigorous enforcement of strict confidentiality agreements with our subcontractors to prevent any unauthorized disclosure of student or staff information they may encounter in their duties. This vigilance in safeguarding educational records and communications is in strict compliance with the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), New York State Education Law §2-d, and Chancellor's Regulation A-820.

To further enhance the security and confidentiality of sensitive information, Stephanie and I are leading an initiative to improve our scheduling portal. This project focuses on incorporating more detailed protocols for the handling and uploading of sensitive documents, ensuring that all security-related information for interpreters and other subcontractors is meticulously managed and accessible in a secure manner, such as through our documents in our training and HR portals. Reflecting NTC's unwavering commitment to confidentiality, it is imperative that our vendors strictly adhere to all applicable federal, state, city, and ESBOCES Regulations concerning confidentiality. This includes a strict prohibition against the release, for commercial purposes, of any information gathered about students, parents/guardians, and employees.

- **Emergency Response and Crisis Communication:** In light of the critical role that communication plays during emergencies, subcontractors are required to have protocols in place for rapid response and crisis communication. This ensures that interpretation and translation services can be quickly mobilized in urgent situations in accordance with ESBOCES guidelines.

By incorporating these specific clauses into our agreements with subcontractors, NTC Language Services ensures a partnership that not only meets the high expectations of ESBOCES but also contributes to an educational environment where every student and family has access to clear, accurate, and culturally sensitive language service.

Monitoring and Evaluation

Subcontractors engaged by NTC Language Services are not merely selected through a rigorous vetting process; they are also subject to a continuous monitoring and evaluation system designed to ensure that their services consistently meet the high standards expected by the company and its clients. This dynamic process involves several key components to maintain and enhance service quality over time.

Firstly, regular feedback sessions are held between subcontractors and management. These sessions are crucial for open communication, allowing subcontractors to share their experiences, challenges, and suggestions for improvement. Conversely, management uses these opportunities to provide constructive



feedback on performance, discuss areas of strength, and identify any areas requiring enhancement. This two-way communication ensures subcontractors align with the company's expectations and quality standards.

Additionally, client satisfaction surveys play a pivotal role in the evaluation process. These surveys are distributed to clients after the completion of a project or at regular intervals for ongoing services. The feedback obtained from these surveys is invaluable, providing insights into the client's perspective on the quality of service received, their satisfaction with the subcontractor's work, and areas where improvements can be made. This direct client feedback is instrumental in assessing the real-world impact of the subcontractors' work and making necessary adjustments.

Performance audits constitute another critical aspect of the ongoing monitoring system. These audits thoroughly review the subcontractors' work against established quality benchmarks and performance metrics. This may include assessing the accuracy and consistency of translations or interpretations, timeliness of service delivery, and adherence to project-specific requirements. Performance audits help identify areas that require immediate attention and trends that may indicate the need for broader changes in training, processes, or subcontractor engagement strategies.

Together, these elements—regular feedback sessions, client satisfaction surveys, and performance audits—form a comprehensive framework for ongoing monitoring and evaluation of subcontractors. This framework not only ensures that subcontractors' services remain at the high standard expected by NTC Language Services but also fosters a culture of continuous improvement, adaptability, and excellence in service delivery. Through this proactive approach to quality assurance, NTC Language Services upholds its commitment to providing exceptional language services that meet and exceed client expectations.

Security Protocols Including Electronic Transmission of Materials

Our adherence to security protocols is a multi-faceted approach that integrates stringent security measures, regular training, and the use of compliant technologies like INTERPRETER INTELLIGENCE. By implementing these protocols diligently, we aim to protect the sensitive information related to students and the school system, and associated services against unauthorized access or disclosure.

Our organization is committed to fully adhering to the outlined Information Security Requirements, ensuring the confidentiality, integrity, and availability of all data handled, especially regarding the electronic transmission of materials. Recognizing the sensitive nature of the data involved with the associated services being provided, we have tailored our approach to meet and exceed these standards, leveraging the Interpreter Intelligence system alongside other cutting-edge technologies.

Our adherence strategy encompasses comprehensive measures aligned with mandates on data classification, privacy, security training, systems administration, and incident response. Firstly, we will implement robust encryption protocols for all data in transit and at rest, ensuring that all electronic transmissions of materials via Interpreter Intelligence for any other technology are secure and inaccessible to unauthorized parties. Interpreter Intelligence, a leading interpretation management system, supports our commitment by offering secure cloud-based solutions that align with global information security standards. This includes regular updates and patches to safeguard against vulnerabilities, alongside stringent access controls and encryption to protect sensitive information.



Moreover, we will conduct regular security training and awareness programs for our team to ensure they are familiar with required security and privacy requirements, as well as best practices for protecting sensitive information. This includes training on the secure use of Interpreter Intelligence and other technologies involved in our processes.

Our systems administration approach will include rigorous change management, patching, and configuration practices to maintain the security integrity of our IT infrastructure. Application development and code review processes will be strengthened by regular static and dynamic code scanning to identify and remediate any potential security flaws.

In terms of incident response, we have a comprehensive plan in place that aligns with all necessary requirements, ensuring swift action and communication in the event of a security breach. This includes immediate containment and eradication procedures, followed by a thorough investigation to prevent future incidents.

Interpreter Intelligence complements our security posture through its compliance with international information security standards. The platform's commitment to regular security assessments and adherence to best practices in application development, data handling, and incident management ensures that it meets the required stringent security protocols.

Report Security

In partnering with ESBOCES, we are fully dedicated to adhering to the stringent guidelines and oversight established. This includes recognizing ESBOCES has authority over all aspects of our service delivery, from the approval of materials and services we provide to the adherence to deliverables schedules.

Central to our operations is a steadfast commitment to maintaining the confidentiality and security of all materials, including examinations, reference materials, and reports. We understand the critical importance of these documents and the sensitive information they contain, which could significantly impact students and their families.

Our organization has implemented a multifaceted information security management system (ISMS) that aligns with globally recognized standards such as ISO/IEC 27001. This standard guides our efforts in identifying, managing, and reducing risks to the security of information, ensuring that sensitive materials are protected against unauthorized access, copying, duplication, or dissemination.

Advanced Electronic Transmission Methods

Our approach to secure electronic transmission of materials incorporates several key technologies and methodologies:

- **End-to-End Encryption (E2EE):** All data transmitted electronically, whether via email or cloud services, is encrypted from the sender's device to the recipient's device, ensuring that data cannot be intercepted and read in transit.
- **Secure File Transfer Protocol (SFTP) and Virtual Private Networks (VPNs):** For the transfer of large files or sensitive data, we use SFTP and VPNs to provide an additional layer of security, ensuring that data is transmitted over encrypted channels.



- **Multi-Factor Authentication (MFA):** MFA is required for accessing our electronic transmission systems, adding an extra verification step that ensures only authorized users can send or receive data.

Encrypted Storage Solutions

For data at rest, we employ robust encrypted storage solutions that include:

- **AES 256-bit Encryption:** All stored data is encrypted using Advanced Encryption Standard (AES) with a 256-bit key, the same level of encryption used by banks and military institutions.

Strict Access Controls

Access to sensitive materials is tightly controlled through:

- **Role-Based Access Control (RBAC):** Access to data is granted based on the individual's role within the organization, ensuring they only have access to information necessary for their duties.
- **Regular Access Reviews:** We conduct periodic reviews of access rights to ensure that only currently authorized individuals have access to sensitive materials.

Clear Communication Protocols

To safeguard against unauthorized discussions of sensitive materials, we have implemented clear communication protocols:

- **Secure Communication Channels:** All internal communications regarding sensitive materials are conducted through encrypted messaging systems.
- **Confidentiality Agreements:** Team members are required to sign confidentiality agreements that explicitly prohibit the unauthorized discussion of sensitive materials.
- **Regular Training:** Employees receive training on the importance of maintaining confidentiality and the proper channels for discussing sensitive information.

Through these specific methods and standards, we ensure a comprehensive and robust approach to information security, safeguarding against any potential breaches while adhering to the necessary requirements.

Please see the next page for additional information about our Data Security and Privacy Plan.



Data Security and Privacy Plan

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, Nuestro Terreno Comun LLC hereby establishes the following data security and privacy plan:

Nuestro Terreno Comun LLC will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as it uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Nuestro Terreno Comun LLC shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Nuestro Terreno Comun LLC shall not use Protected Data for any other purposes than those explicitly provided for in its agreement with the disclosing party from which it received Protected Data. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Nuestro Terreno Comun LLC shall have in place sufficient internal controls to ensure that Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by a customer. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of an educational agency as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),

-AND-

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-c218147

State, federal, and local data security and privacy contract requirements will be implemented by utilizing Best practices and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff shall be implemented as follows:

All computer equipment is inventoried and distributed by the managing members of the LLC. It is physically secured using lock and key. Our servers are equipped with firewalls and password protections. Staff are provisioned accounts by the company's President and Vice President and access is limited through paths providing staff with limited password protected access. Word processing documents are also encrypted as necessitated by ED Law. When transmitted, data is either encrypted on physical medium, such as a USB drive, or transmitted over a secure

**EASTERN SUFFOLK BOCES
PARENTS' BILL OF RIGHTS
FOR DATA SECURITY AND PRIVACY**

Eastern Suffolk BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information. The Agency wishes to inform the school community of the following rights:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record maintained by Eastern Suffolk BOCES.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available for public review at: <http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>, Or, by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Claudy Damus-Makelele
Associate Superintendent for Educational Services
Eastern Suffolk BOCES
201 Sunrise Highway
Patchogue, NY 11772
cdamus@esboces.org

Or in writing to:

Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, New York 12234.
CPO@mail.nysed.gov

Supplemental Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract the Agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;
Answer: The successful vendor needs to confirm that any and all data (including student, teacher, and principal data) is not to be used for any purpose, other than the encryption of that data.
2. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;

Answer: The successful vendor will be required in the bid process to describe how they will abide by data protection and security requirements.

3. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;

Answer: The successful vendor will be required in the bid process to describe how they will abide by data protection and security requirements at the expiration of the agreement.

4. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and

Answer: Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

*Claudy Damus-Makelele, Associate Superintendent for Educational Services Eastern
Suffolk BOCES, 201 Sunrise Highway, Patchogue, NY 11772
cdamus@esboces.org;*

Or in writing to:

*Chief Privacy Officer, New York State Education Department, 89 Washington Avenue
Albany, NY 12234
CPO@mail.nysed.gov*

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

Answer: The successful vendor will be required in the bid process to describe how they will ensure data is encrypted and protected.

Third Party Contractors are required to:

1. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
2. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
3. Not use educational records for any other purpose than those explicitly authorized in the contract;
4. Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

5. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
6. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
7. Notify Eastern Suffolk BOCES of any breach of security resulting in an unauthorized release of student data or teacher or principal data, in the most expedient way possible and without unreasonable delay;
8. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
9. Provide a signed copy of this Bill of Rights to Eastern Suffolk BOCES thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

A copy of this ESBOCES Parents' Bill of Rights must be made a part of Contractor's Data Security and Privacy Plan.

The following has been pulled from the Parents' Bill of Rights section in the Education Law 2-d Rider packet. Please review and answer questions 1, 2, 3 and 5.

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services, Eastern Suffolk BOCES has entered into contracts with certain third-party contractors. Pursuant to such contracts, third-party contractors may have access to "student data" and/or "teacher or principal data." Each contract Eastern Suffolk BOCES enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data will include information addressing the following:

1. The exclusive purposes for which the student data or teacher or principal data will be used;

The following purposes for which student data, or teacher, or principal data may be used include, but are not limited to:

Translation Services: To accurately translate educational materials, records, and communications from one language to another, ensuring that non-English speaking students and their families have access to the same information as their English-speaking peers.

Interpretation Services: To provide real-time or scheduled interpretation services during parent-teacher conferences, school meetings, and other educational events to facilitate effective communication between school staff and non-English speaking parents or guardians.

Educational Support: To assist in the creation of multilingual educational resources, such as instructional materials, homework assignments, and assessments, ensuring that all students receive equitable access to education.

Compliance with Legal Requirements: To ensure compliance with federal and state laws regarding language access in education, such as the Individuals with Disabilities Education Act (IDEA) and Title VI of the Civil Rights Act, which mandate that schools provide language assistance to non-English speaking students and their families.

Confidentiality and Security: To maintain the confidentiality and security of personally identifiable information in accordance with applicable laws and regulations, such as FERPA and Education Law 2-d, ensuring that data is used solely for the purposes of providing translation and interpretation services and is not disclosed to unauthorized parties.

Customized Educational Plans: To assist in the development and implementation of Individualized Education Programs (IEPs) and other customized educational plans for students who require special accommodations, ensuring that these plans are effectively communicated to non-English speaking parents and guardians.

Professional Development: To provide training and resources for teachers and school staff on best practices for working with multilingual students and their families, using data to tailor the training to specific needs and contexts.

Parental Engagement: To enhance parental engagement by translating newsletters, notices, and other school communications, ensuring that non-English speaking parents are fully informed and can participate in their child's education.

Cultural Competency: To support schools in fostering a culturally inclusive environment by translating materials that promote cultural awareness and sensitivity, and by interpreting during

events that celebrate cultural diversity.

Crisis Communication: To provide timely and accurate translation and interpretation services during emergencies or critical incidents, ensuring that all students and their families receive important information and instructions.

Feedback and Surveys: To translate and interpret feedback forms, surveys, and other tools used to gather input from students, parents, and staff, ensuring that the voices of non-English speakers are heard and considered in school decision-making processes.

Compliance Monitoring: To assist schools in monitoring and reporting compliance with language access requirements, using data to demonstrate adherence to legal and policy standards.

Support Services: To facilitate communication between non-English speaking students and school support services, such as counseling, health services, and extracurricular activities, ensuring that all students have access to the full range of school resources.

Documentation and Record Keeping: To accurately translate and interpret student records and documentation, ensuring that all educational records are complete and accessible to authorized personnel and parents, regardless of language barriers.

Any data which may need to be used will be first presented to the appropriate school contact for approval when needed.

2. How the third-party contractor will ensure that the subcontractors, persons, or entities with whom the third-party contractor will share the student data or teacher or principal data, if any, will abide by data protection and security requirements;

For the purposes of this specific contract, we will not be utilizing subcontractors to perform direct services. If there is a point where NTC Language Services utilizes subcontractors we will ensure that subcontractors, persons, or entities with whom they share student data, teacher data, or principal data abide by data protection and security requirements through the following measures:

Contractual Obligations: NTC Language Services includes specific data protection and security clauses in all contracts with subcontractors. These clauses will outline the subcontractors' obligations to protect personally identifiable information (PII) in compliance with relevant laws and regulations, such as FERPA, Education Law 2-d, and other applicable state and federal privacy laws.

Data Security and Privacy Policies: NTC provides subcontractors with our data security and privacy policies, ensuring that subcontractors understand and agree to adhere to these policies. These policies cover administrative, technical, and physical safeguards to protect PII.

Access Controls: NTC implements strict access controls to ensure that only authorized subcontractors and personnel have access to PII. Access is granted based on the principle of least privilege, meaning that individuals will only have access to the data necessary to perform their specific job functions.

Monitoring and Auditing: NTC conducts regular monitoring and auditing of subcontractors to ensure compliance with data protection and security requirements. This includes periodic reviews of subcontractors' data handling practices and security measures.

Incident Response and Reporting: NTC has established clear procedures for subcontractors to report any data breaches or security incidents. Subcontractors will be required to promptly notify NTC of any unauthorized access or disclosure of PII, and NTC will work with them to address and mitigate the impact of such incidents.

Encryption and Data Protection Measures: NTC requires subcontractors to use encryption and

other data protection measures to secure PII both in transit and at rest. This helps prevent unauthorized access and ensure the confidentiality and integrity of the data.

Non-Disclosure Agreements (NDAs): NTC requires subcontractors to sign NDAs that legally bind them to maintain the confidentiality of PII and prohibit unauthorized use or disclosure of the data.

Termination and Data Deletion: Upon the termination of the contract or agreement, NTC ensures that subcontractors securely delete or return all PII in their possession. Subcontractors will be required to provide certification of data deletion or return to confirm compliance.

Compliance with Laws and Regulations: NTC ensures that subcontractors comply with all applicable laws and regulations governing data protection and privacy. This includes adhering to the requirements set forth in Education Law 2-d and other relevant legal frameworks.

3. When the contract expires and what happens to the student data or teacher or principal data upon expiration of the contract;

When the contract with NTC Language Services expires, the following procedures will be followed regarding student data, teacher data, or principal data:

Data Deletion or Return: Upon the expiration of the contract, NTC Language Services will either securely delete or return all student data, teacher data, or principal data in their possession. The specific action will depend on the terms agreed upon in the contract and the preferences of the educational agency.

Secure Transmission: If the data is to be returned, it will be transmitted securely to the educational agency using encryption or other secure methods to ensure the confidentiality and integrity of the data during transfer as per current industry encryption standards.

Certification of Deletion: If the data is to be deleted, NTC Language Services will provide a formal certification of data deletion. This certification will include details such as the date of deletion, the method used for deletion, and a confirmation that all copies of the data have been securely erased.

Verification of Deletion: NTC Language Services will implement verification procedures to ensure that the data deletion process is complete and thorough. This may involve audit logs, deletion reports, and possibly third-party verification to confirm that no residual data remains.

Compliance with Legal and Contractual Obligations: All actions taken to delete or return data will be in strict compliance with applicable data protection laws and regulations, including Education Law 2-d, FERPA, and any other relevant legal requirements. Additionally, NTC will adhere to any specific contractual obligations related to data handling upon contract expiration.

Notification to Client: NTC Language Services will notify the educational agency once the data has been securely deleted or returned. This notification will include the certification of deletion or confirmation of data return, along with any relevant documentation.

Retention of Minimal Data for Legal Purposes: If required by law, NTC Language Services may retain minimal data necessary for legal, regulatory, or compliance purposes. Any retained data will be securely stored and protected in accordance with data protection standards until it is no longer needed.

4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected;

Complaints should be directed to: the Associate Superintendent for Curriculum for your district;
Or in writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234, CPO@mail.nysed.gov.

5. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security) and the security protections taken to ensure that such data will be protected, including whether such data will be encrypted.

If NTC Language Services will store data, it will be stored in a secure manner, employing robust security protections to ensure the confidentiality, integrity, and availability of the data. The following describes where the data will be stored and the security measures taken:

Data Storage Locations

Secure Servers: The data stored on secure servers located in data centers that comply with industry standards for physical and digital security

Cloud Storage: If cloud storage is used, it is provided by reputable cloud service providers that offer advanced security features. These providers comply with relevant data protection regulations and standards, such as SOC 2, ISO 27001, and GDPR.

Security Protections

Encryption

Data in Transit: All data transmitted between NTC Language Services and its clients, as well as between internal systems, is encrypted using secure protocols such as TLS (Transport Layer Security) to prevent unauthorized access during transmission.

Data at Rest: Data stored on servers or in cloud storage is encrypted using strong encryption algorithms (e.g., AES-256) to protect it from unauthorized access.

Access Controls

Role-Based Access Control (RBAC): Access to data is restricted based on the principle of least privilege. Only authorized personnel with a legitimate need to access the data are granted permissions, and their access will be limited to the minimum necessary to perform their job functions.

Multi-Factor Authentication (MFA): MFA is provided for accessing systems that store or process sensitive data, adding an extra layer of security beyond just passwords.

Physical Security

Data Centers: The physical security of data centers include measures such as 24/7 surveillance, access controls, biometric authentication, and security personnel to prevent unauthorized physical access.

Network Security

Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS): Firewalls and IDS/IPS will be

used to monitor and protect the network from unauthorized access and potential threats.

Segmentation: Network segmentation will be employed to isolate sensitive data and systems from less secure parts of the network, reducing the risk of unauthorized access.

Data Backup and Recovery

Regular Backups: Regular backups of data are performed to ensure that data can be restored in the event of data loss or corruption. Backups are encrypted and stored securely.

Disaster Recovery Plan: A comprehensive disaster recovery plan is in place to ensure business continuity and data availability in case of a major incident.

Monitoring and Auditing

Continuous Monitoring: Systems will be continuously monitored for suspicious activity, unauthorized access attempts, and potential security breaches.

Regular Audits: Regular security audits and assessments are conducted to identify and address vulnerabilities and ensure compliance with security policies and regulations.

Compliance with Legal and Regulatory Standards:

NTC Language Services complies with all relevant data protection laws and regulations, including Education Law 2-d, FERPA, and other applicable federal and state laws. This compliance ensures that data security measures meet or exceed legal requirements.