CONTRACT ADDENDUM

Protection of Personally Identifiable Information

1 .Applicability of This Addendum

The Greater Southern Tier B.O.C.E.S. ("DISTRICT") and Body Interact Inc ("Vendor") are parties to an agreement (contract) dated December 27, 2024 governing the terms under which DISTRICT accesses, and Vendor provides, products Body Interact. DISTRICT's use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify any existing contracts and shall have precedence over any online Terms of Use or Service published by Vendor.

2. Definitions

2.1 "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from DISTRICT or is created by the Vendor's product or service in the course of being used by DISTRICT.

2.2 "Vendor" means the vendor identified above.

2.3 "Educational Agency" means a school district, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes DISTRICT.

2.4 “DISTRICT" means the Greater Southern Tier B.O.C.E.S.

2.5 "Parent" means a parent, legal guardian, or person in parental relation to a Student.

2.6 "Student" means any person attending or seeking to enroll in an educational agency.

2.7 "Eligible Student" means a student eighteen years or older.

2.8 "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9 "This Contract" means the underlying Master Agreement (contract) as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a

school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the DISTRICT Data Security and Privacy Policy and Parent’s Bill of Rights for Data Privacy and Security, which are included in this document.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes Vendor warrants that Protected Information received by Vendor from DISTRICT or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

a. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with DISTRICT. Vendor shall acquire no ownership interest in education records or Protected Information.

b. DISTRICT shall always have access to the DISTRICT's Protected Information through the term of this Contract. DISTRICT shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

c. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by DISTRICT or its authorized users or performing any other data analytics other than those required to provide the Product to DISTRICT. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to DISTRICT upon request.

d. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All help desk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to DISTRICT.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase , lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share

Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

a. The expiration date of this Contract is defined by the underlying Master Agreement (contract).

b. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist DISTRICT in exporting all Protected Information previously received from, or then owned by DISTRICT.

c. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities .

d. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

e. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

f. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to DISTRICT from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

a. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the DISTRICT for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

b. Vendor will cooperate with DISTRICT in retrieving and revising Protected Information but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

a. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the District’s Data Security and Privacy Plan as set forth in this addendum .

b. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

i. align with the NIST Cybersecurity Framework 1.0;

ii. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

iii. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the DISTRICT data security and privacy policy as set forth in this addendum.

iv. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

v. demonstrate that it complies with the requirements of Section 121.3(c) of this Part; specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access ;

vi. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected; vii. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify DISTRICT; and

viii. describe whether, how and when data will be returned to DISTRICT, transitioned to a successor contractor, at DISTRICT's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. Additional Vendor Responsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

a. Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

b. Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

c. Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the DISTRICT unless (i) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure

is required by statute or court order, and notice of the disclosure is provided to DISTRICT no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

d. Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

e. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

f. Vendor will notify the DISTRICT of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

g. Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse DISTRICT for the full cost incurred by DISTRICT to send notifications required by Education Law Section 2-d.

14. The District's Data Security and Privacy Policy, referenced herein, is as follows:

DATA SECURITY AND PRIVACY POLICY

The BOCES will comply with and implement the provisions of the Family Educational Rights and Privacy Act (FERPA), Education Law §§ 2-d, 101, 305 and their implementing or related regulations.

In particular, the BOCES will, in complying with and implementing these laws and regulations, take the following actions regarding the personally identifiable information of its students, parents, and staff:

1. The BOCES will not sell such personally identifiable information nor use it or allow it to be used for any marketing or commercial purpose and will minimize the collection, processing, and transmission of such information.

a. The BOCES will ensure that it has provisions in its contracts with third-party contractors that require that the confidentiality of such personally identifiable information be maintained.

b. The BOCES shall not report to NYSED juvenile delinquency, criminal, or medical and health records, or biometric information of its students, except as required by law.

2. The BOCES will publish on its website a parents' bill of rights for data privacy and security which is attached to this policy and that complies with the requirements of 8 NYCRR Part 121.

a. This parents' bill of rights will include certain provisions regarding such personally identifiable information that each third party contract must contain, include the purpose that any such personally identifiable information will be used, how subcontractors will abide by all data security and privacy requirements, the duration of the contract, how a parent, student or staff member may challenge the accuracy of any such personally identifiable data that is used, where such personally identifiable information will be stored and the precautions taken to protect such information, and how the information will be encrypted while it is in motion.

b. Such provisions will be published on the BOCES' website and may be redacted in accordance with the law and regulations.

3. Procedures for individuals to file complaints about breaches or unauthorized releases of such personally identifiable information will be established and communicated.

a. As part of these procedures, the BOCES will acknowledge receipt of complaints, commence and investigation, and take necessary precautions to protect such personally identifiable information.

b. The BOCES will provide the complainant with its findings within 60 days from the receipt of the complaint.

c. The BOCES will maintain a record of all such complaints.

4. The BOCES adopts the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Cyber Security Framework or NIST CSF) as its standard for data security and privacy.

5. Every use and disclosure of such personally identifiable information by the BOCES shall benefit students and the BOCES. Such personally identifiable information shall not be included in public reports or other documents.

6. A copy of this policy shall be published on the BOCES' website and all notice of the policy will be provided to all BOCES' officers and employees.

7. Each third-party contract entered into by the BOCES shall include the third-party contractor's data security and privacy plan, which shall:

a. Outline how the third-party contractor will comply with state, federal, and local data privacy and security laws, regulations, and polices regarding protection of such personally identifiable information.

b. Specify the safeguards and practices that the contractor has in place to protect such personally identifiable information.

c. Specify how training on the federal and state laws regarding privacy of such personally identifiable information will occur.

d. Specify how subcontractors will be managed to ensure such personally identifiable information will be protected.

e. Specify how incidents involving breaches or unauthorized disclosures of such personally identifiable information will be identified and managed, and how the BOCES will be notified in the event of such breach or disclosure.

f. Specify how data will be returned to the BOCES or deleted or destroyed at the termination or expiration of the contract.

8. The BOCES shall annually provide data security awareness training to their officers and employees with access to such personally identifiable information in accordance with 8 NYCRR Part 121.

9. The BOCES shall designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law § 2-d and 8 NYCRR Part 121, and to serve as the point of contact for data security and privacy of the BOCES.

10. The BOCES shall ensure that all third-party contractors shall be in compliance with the requirements of 8 NYCRR 121.9.

11. Breaches and unauthorized releases of such personally identifiable information.

a. Third-party contractors shall promptly notify the BOCES of any breach or unauthorized release of such personally identifiable information.

b. The BOCES shall report every discovery or report of a breach or unauthorized release of such personally identifiable information to the New York State Chief Privacy Officer within 10 calendar days after such discovery.

c. The BOCES shall notify the person whose personally identifiable information (and/or the parent of such person, if they are a student) was compromised by such breach or unauthorized release within 60 calendar days after such discovery.

d. Persons who believe that their personally identifiable information, or that of their child, if they are a parent, has been compromised shall so notify the BOCES of such breach or unauthorized release.

12. Parents and eligible students may inspect and review student educational records by making a written request to the BOCES.

a. The BOCES shall verify the identity of the requestor before releasing any information.

b. The BOCES shall notify parents annually of their right to inspect and review their child's educational records. The annual notice required pursuant to FERPA shall be deemed to satisfy this requirement.

c. The BOCES shall comply with a request for access to records within 45 calendar days after receipt of a request.

13. Any other requirements of the New York State Education Law, the New York State Regulations, or FERPA or its federal implementing regulations regarding data privacy and security not mentioned in this policy shall be complied with and shall take precedence over any provision in this policy, and all requirements of said laws and regulations shall be complied with in the manner proscribed in said law or regulation, notwithstanding anything contained in this policy to the contrary.

15. The District's Parent's Bill of Rights for Data Privacy and Security, referenced herein, is as follows:

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

a. A student or staff member's personally identifiable information cannot be sold or released for any commercial purposes.

b. Parents have the right to inspect and review the complete contents of their child's education record.

c. 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.

d. A complete list of all student data elements collected by New York State is available for public review at the following website http://www.nysed.gov/student-dataprivacy/student-data-inventory or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

e. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Data Privacy Officer, Computer Services Center, GST BOCES, 459 Philo Road, Elmira, NY 14903.

16. The Vendor agrees to protect the protected information of the students, teachers, and principals of GST BOCES by addressing the following issues in the following manner:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, are as follows:

Body Interact will access Personally Identifiable Information (PII) — specifically, first name, last name, school email address, and IP address (for mobile access) — exclusively for the following purposes:

a. Student Performance Tracking: to enable personalized feedback and progress monitoring, helping educators assess student development.

b. Platform Usage Analytics: to support educators and administrators in evaluating simulation engagement and usage.

c. Technical Support: to resolve platform access, functionality, or other performance or technical issues as needed.

2. **How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d) is as follows:**

Body Interact relies on established, reputable cloud service providers for its infrastructure and hosting services. These providers offer robust security features and certifications that are leveraged to ensure the protection of Protected Information. Body Interact has reviewed the privacy and security policies of these providers and determined that they align with the terms of this NDA, ensuring equivalent data security and confidentiality requirements.

Key aspects of managing the relationship with these Cloud providers include:

- **Compliance with Industry Standards**: Providers are certified under globally recognized standards such as ISO 27001, ensuring adherence to high data security standards.
- **Data Protection Policies**: Built-in data protection measures, including encryption, access controls, and compliance with global data protection regulations, are utilized to secure Protected Information.
- **Risk Mitigation**: Body Interact ensures proper configuration and use of the providers' security features to protect data, regularly monitoring and addressing potential risks.

Body Interact is committed to implementing all applicable state, federal, and local data security and privacy contract requirements throughout the life of the agreement. The following measures have been put into place:

- **Compliance with Federal and State Laws**:

  Compliance with all relevant federal and state data privacy laws, including but not limited to:
  - **FERPA (Family Educational Rights and Privacy Act)**, which protects the confidentiality of student education records.
  - **New York State Education Law §2-d**, which mandates data privacy and security protections for student data in New York.
  - **The NY SHIELD Act**, which requires robust safeguards for personal information and breach notification.

3. **The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed); is as follows:**

The contract has a duration of one year, from November 4, 2024 to November 3, 2025.

Body Interact is committed to ensuring the secure handling of Protected Information at the conclusion of the contract, in accordance with the DISTRICT requirements. Our practices are as follows:

1. **Data Deletion and Destruction**:
   Upon the occurrence of any specified event (e.g., at the DISTRICT's request, cessation of service use, or termination of the agreement), all respective data stored in our systems will be securely deleted. This process utilizes approved electronic file destruction methods to ensure the data is irrecoverable.

2. **Certification of Destruction**:
   Following the completion of the data deletion process, we will issue a "Certificate of Records Disposal" to the DISTRICT, confirming that all Protected Information has been securely destroyed.

3. **Data Retention Timeline**:
   Protected Information will not be retained beyond one school year after the year in which it was received, unless explicitly required by law or directed otherwise by the DISTRICT.

4. **Physical Records**:
   We do not retain physical copies of Protected Information. Therefore, the physical destruction of records does not apply.

4. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; is as follows

Personally Identifiable Information (PII) will be stored or hosted using a cloud or infrastructure owned tool hosted by a subcontractor; i.e., Microsoft Azure.

Administrative, technical, and physical safeguards have been implemented to protect PII. These measures are certified under ISO 27001, an internationally recognized standard for information security management, demonstrating a commitment to maintaining high standards for data security, privacy, and integrity. This certification covers all aspects of the product lifecycle, including specification, design, production, quality assurance, and post-delivery activities, along with all processes involving the handling of sensitive information

Administrative safeguards include strict access controls and data privacy policies that limit PII access to authorized personnel only, in accordance with data privacy regulations and organizational policies. Technical safeguards involve the encryption of data both in transit and at rest, along with continuous monitoring, intrusion detection, and security patch management to ensure resilience against cybersecurity threats. Physical safeguards include secure facilities with controlled access to prevent unauthorized physical access to systems processing PII.

Additionally, regular risk assessments and audits are conducted to identify, manage, and mitigate any data privacy and security risks proactively, ensuring ongoing compliance with ISO 27001 standards and a steadfast commitment to protecting sensitive data.

5. **The data will be protected using encryption while in motion and at rest as follows:**

Protected Information is encrypted both at rest and in transit using industry-standard encryption protocols. Access to encryption keys is restricted to authorized personnel.

6. The Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and will promptly notify DISTRICT of any such breaches or unauthorized disclosures, as follows:

The management of data security and privacy incidents is conducted in accordance with the product's ISO 27001-certified Information Security Management System (ISMS). The following measures are implemented to ensure proper handling of incidents involving Protected Information:

1. **Incident Detection and Response**:

Body Interact employs advanced monitoring tools and procedures to promptly identify potential breaches or unauthorized disclosures. Upon detection of an incident, a defined process is followed to contain the issue, conduct a thorough investigation, and implement mitigation strategies to minimize impact.

Responsabilities:

- **CISO (Chief Information Security Officer)**: Oversees incident response, ensuring adherence to ISMS protocols.
- **IT Operations Team**: Investigates technical aspects of the incident, such as system logs and network activity, to identify the source and scope.
- **Executive Management**: Reviews the incident's impact and approves key decisions on mitigation and communications.

2. **Notification to DISTRICT**:

If a data breach involving Protected Information is confirmed, the DISTRICT will be notified within 24 hours. This notification will include detailed information about the nature of the breach, steps taken to address the incident, and measures being implemented to prevent similar occurrences in the future.

Responsibilities:

- **CISO**: Coordinates and drafts the breach notification.
- **Executive Management**: Approves the final communication before it is sent to the DISTRICT.

3. Post-Incident Improvements:

Following the resolution of any incident, a root cause analysis is performed to identify vulnerabilities or process gaps. Based on these findings, corrective actions are implemented to continuously enhance our data security practices.

Responsibilities:

- **CISO**: Leads the root cause analysis, documents findings, and updates risk assessments and controls within the ISMS.
- **IT Operations Team**: Implements technical corrective measures based on analysis.

The product’s ISO 27001 certification ensures compliance with industry best practices for incident management and data protection. This certification reinforces our commitment to maintaining the highest standards of security and privacy.

Signatures

For The Vendor:

Signature: 

Printed Name: Pedro Pinto

Title: President

Contact Information: pedropinto@bodyinteract.com

Date: December 27, 2024

For The District:

Signature: Edward R White III

Printed Name: Edward White III

Title: Data Protection Officer

Contact Information: DPO@gstboces.org

Date: 5/2/2025