ImPACT Applications, Inc.
New York Education Law 2-d Rider

New York State Education Law § 2-d ("Education Law 2-d") was enacted in 2014 to address concerns relating 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 the New York Parents' Bill of Rights concerning the protection data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and ensuring that each third-party contractor signs a copy of the educational agency's Parents' Bill of Rights. This New York Education Law 2-d Rider (the "**Agreement**") enumerates the requirements that a third-party contractor must satisfy to comply with the Parents' Bill of Rights. This Agreement is made subject to and incorporates by reference the **VENDOR**'s Terms of Use (https://impacttest.com/terms-of-use/) and Privacy Notice (https://impacttest.com/privacy-notice/). If there is a conflict between the Terms of Use and/or Privacy Notice and this Agreement, this Agreement will control.

This Agreement will begin on the latest date set forth on the signature page ("**Effective Date**") and will expire upon termination of the underlying Services Agreement. A copy of the applicable Parents' Bill of Rights is attached hereto as Attachment A. Supplemental information about **VENDOR's** services and a schedule of the data collected by these services is attached hereto as Attachment B.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Terms of Use between Central Islip UFSD ("**DISTRICT**") and ImPACT Applications, Inc. ("**VENDOR**") to the contrary, **VENDOR** agrees as follows:

Definitions

"**Personally identifiable information**" means student records of the **DISTRICT** as that term is defined in §99.3 of FERPA. Personally identifiable information from the records of the **DISTRICT** relating to the annual professional performance reviews of classroom teachers or principals is confidential and not subject to release under the provisions of Education Law 3012-c.

"**Protected Data**" means any information rendered confidential by state or federal law, including student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the **DISTRICT**. Protected Data does not include de-identified data. Protected Data also includes any information protected under Education Law 2-d.

Purpose

VENDOR will receive Protected Data from the **DISTRICT** for purposes of providing certain online tools for baseline and post-injury testing relating to the assessment and management of concussions.

Confidentiality, Breach & Return/Destruction of Data

VENDOR will treat Protected Data as confidential and will protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as **VENDOR** uses to

protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. **VENDOR** 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. **VENDOR** 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, **VENDOR** shall have in place sufficient internal controls designed to ensure that the **DISTRICT**'s Protected Data is safeguarded in accordance with all applicable laws and regulations, including the Children's Internet Protection Act, the Family Educational Rights and Privacy Act ("**FERPA**") and the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), as applicable.

Any subcontractor, affiliate, or entity that may receive, collect, store, record, or display any Protected Data on behalf of **VENDOR** will substantially comply with Education Law 2-d by contractual obligation to **VENDOR**. Subject to the limitation of liability set forth in the Terms of Use, **VENDOR** will promptly reimburse **DISTRICT** for the cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by **VENDOR** or its subcontractors that results from **VENDOR**'s breach of its obligations under this Agreement. If this Agreement expires, is not renewed, or is terminated, **VENDOR** shall, within thirty (30) days' after receiving written notice from **DISTRICT** and subject to the consent of any entity that pays for or otherwise sponsors **DISTRICT**'s use of **VENDOR**'s services, such as an insurance company or state educational agency, return **DISTRICT** data, including any and all Protected Data, in its possession by secure transmission or will delete all Protected Data as directed by **DISTRICT**. Notwithstanding the foregoing, **VENDOR** may retain data to the extent permitted by law or otherwise technically infeasible of return, including backups, which will be retained and expire in accordance with **VENDOR**'s backup retention and restoration policies.

Data Security and Privacy Plan

VENDOR maintains a Data Security and Privacy Plan, attached hereto as Attachment C, that complies with the requirements of New York Education Law § 2-d and Part 121 of the Regulations of the Commissioner of Education.

CENTRAL ISLIP UFSD	**IMPACT APPLICATIONS, INC.**
Philip Voigt	DocuSigned by: Tyler Morrison A5CDEDB3C063486...
Signature	Signature
Phil Voigt/Director of Technology	Tyler Morrison SVP Clinical Transformation
Printed Name and Title	Printed Name and Title
December 4th	Dec-04-2023
Date	Date

Attachment A

Parents' Bill of Rights for Data Privacy & Security

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

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law § 2-d and 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 may not apply to parents of a student defined as an Eligible Student (a student 18 years and older).

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, 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); 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 http://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. Complaints may be submitted to NYSED at http://www.nysed.gov/data-privacysecurity/report-improper-disclosure by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to: privacy@nsed.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.

10. Parent have the right to submit complaints about possible breaches of student data or teacher or principal APPR data. Any such complaint must be submitted, in writing to:

Attachment B

Supplemental Information & Schedule of Data

A. Supplemental Information

SUPPLEMENTAL INFORMATION ELEMENT	SUPPLEMENTAL INFORMATION
Please list the exclusive purpose(s) for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract (or list the section(s) in the contract where this information can be found)	ImPACT, an online concussion management tool for baseline and post-injury testing, measures visual and verbal memory, reaction time, and processing speed to help determine if a student (ages 12 and up) can safely return to activity.
Please list how the contractor will ensure that any other entities with which it shares the protected data, if any, will comply with the data protection and security provisions of law, regulation and this contract (or list the section(s) in the contract where this information can be found)	Contractor will store and process protected data in accordance with industry standards, including appropriate administrative, physical, and technical safeguards, to secure protected data from unauthorized access, disclosure, alteration and use.
Please list when the agreement expires and what happens to the protected data when the agreement expires (or list the section(s) in the contract where this information can be found)	Upon written request of the Client, subject to ImPACT Applications internal backup data retention policies and except as required under applicable law, regulation, court order, subpoena, or similar legal process contractor will delete the protected data.
Please list how a parent, student, or eligible student may challenge the accuracy of the protected data that is collected; if they can challenge the accuracy of the data, describe how (or list the section(s) in the contract where this information can be found)	A parent or guardian, student, teacher or principal can challenge the accuracy of the Data received by the Consultant by following applicable law (e.g., Family Educational Rights and Privacy Act).
Please list where the protected data will be stored (described in a way that protects data security), and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated (or list the section(s) in the contract where this information can be found)	All server infrastructure is housed in a secure datacenter facility, in a private locked rack. Only authorized users are allowed to access the environment. 24x7x365 video monitoring, multi-factor access system is in place, UPS, generator and fire protection systems all in place and tested routinely. Production facilities are in Pittsburgh, PA and Disaster Recovery is in Los Angeles, CA.
Please list how the data will be protected using encryption (or list the section(s) in the contract where this information can be found)	PII is encrypted at rest using AES 128-bit encryption. All database backup files are encrypted with AES 256-bit encryption prior to being transmitted from the database server. All data in transit between the end user and contractor systems are encrypted using HTTPS transactions, at the highest level of encryption negotiated by the end user's browser, a minimum of 128-bit.

B. Schedule of Data

Application Technology Meta Data	**IP Addresses, Use of cookies etc.**	**x**
	Other application technology meta data Specify:	
Application Use Statistics	**Meta data on user interaction with application**	
Assessment	**Standardized test scores**	
	Observation data	
	Other assessment data (specify): *Student Personality Assessments*	
Attendance	**Student school (daily) attendance data**	
	Student class attendance data	
Communication	**Online communications that are captured (emails, blog entries)**	
Conduct	**Conduct or behavioral data**	
Demographics	**Date of Birth**	**x**
	Place of Birth	
	Gender	**x**
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	**x**
	Other demographic information Specify:	
Enrollment	**Student school enrollment**	
	Student grade level	(optional)
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information (specify):	
Parent/Guardian Contact Information	**Address**	(optional)
	Email	
	Phone	
Parent/Guardian ID	**Parent ID number (created to link parents to students)**	
Parent/Guardian Name	**First and/or Last**	
Schedule	**Student scheduled courses**	(optional)
	Teacher names	
Special Indicator	**English language learner information**	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information(specify): *First Generation College Student*	

Student Contact Information	**Address**	(optional)
	Email	(optional)
	Phone	
Student Identifiers	**Local (School district) ID number**	
	State ID number	
	Vendor/App assigned student ID#	
	Student app username	
	Student app passwords	
Student Name	**First and/or Last**	**x**
Student In-App Performance	**Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)**	**x**
Student Program Membership	**Academic or extracurricular activities a student may belong to or participate in**	
Student Survey Responses	**Student responses to surveys or questionnaires**	
Student work	**Student generated content; writing, pictures etc.**	
	Other student work data Please specify:	
Transcript	**Student course grades**	
	Student course data	
	Student course grades/performance scores	
	Other transcript data Please specify:	
Transportation	**Student bus assignment**	
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data Please specify:	
Other	**Please list each additional data element used, stored or collected by your application**	*****See below**

***Required: ADD/ADHD diagnosis, Learning disability diagnosis, concussion within the last 6 months.

Optional: Received speech therapy, Attended special education classes, Repeated one or more years of school, Type of student, Current sport, position and level of Number of times diagnosed with a concussion, Number of concussions that resulted in – loss of consciousness, confusion, difficulty remembering events before / after injury, number of games missed as a direct result of concussions, Been treated by a physician for: headaches, migraine headaches, epilepsy/seizures, brain surgery, meningitis, substance/alcohol abuse, psychiatric condition (depression/ anxiety), Diagnosed with dyslexia, autism, Participated in strenuous exercise within the last 3 hours, Hours of sleep last night, Current medications.

Attachment 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.	ImPACT Applications has implemented many policies and procedures as it relates to the security, privacy and availability of our application environments. We undergo annual SOC 2 Type II audits by an independent third-party auditor covering the domains of security, privacy and availability. ImPACT Applications has also achieved ISO 13485 certification for our quality management system. We've also ensured HIPAA Privacy and Security rule compliance.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Administrative, physical and technical safeguards, in congruence with HIPAA's privacy and security rules are part of our company's quality management system and are ingrained in the normal business operations practices. Risk analysis, access control and authorization, physical facility access policies, data backup and encryption all are part of policies that are in place.
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.	Employees receive training on data privacy and security, HIPAA compliance, various cybersecurity topics and many other internal training courses that are relevant to the employee's job position. These training courses are assigned by the Director of Regulatory Affairs and are tracked through an online system to ensure employee compliance.
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.	Employees are required to read and acknowledge our employee handbook, as well as several other employment related documents upon the start of their employment with the company. Employment doesn't start until all of these agreements are signed.

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.	Any data security and privacy incidents will undergo discovery and risk assessment, identification of the cause and extent of the breach, foreseeable harm of the breach, and notification of affected customers. Notification to affected customers will occur within 48 hours of becoming aware of the breach.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Customers are able to export their data at any time via the ImPACT Applications Customer Center.
7	Describe your secure destruction practices and how certification will be provided to the EA.	When a machine or hard drive is decommissioned and has been used by an employee with access to Personal Information, the drive must be securely erased or destroyed before the machine, or its hard drive can be relinquished from the company's control. DBAN is our utility of choice, a disk image for a bootable CD can be found at https://dban.org. If the drive has failed, and will not complete a DBAN destruction attempt, the drive must be physically destroyed so the platters inside are crushed, and it is not usable any longer. Document template QT-18 is to be used to create a record of the data destruction, signed, and stored as evidence of the completed action. Data deleted from our production databases as part of our data deletion processes is identified and removed based on the age of the records, and the data retention settings of the customer organization. Data is removed by an automated process, executing sql statements to remove the specified information from our online databases. The number of records before and after a data deletion event can be provided to confirm the removal of data.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Our data security practices were designed to meet and exceed the requirements set by HIPAA and many other state/local entities. Our policies and procedures have been audited as part of our ISO 13485 certification and SOC 2 Type 2 annual audits.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

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.	Our systems are housed in a secure datacenter facility, within a locked cabinet. Only authorized employees have access to the computing environment. Access to environments (physical or logical) must be approved by management and allocated to each individual user. Hardware assets are tracked by serial number. The company follows a joiners & leavers process to ensure accounts are provisioned and deprovisioned in a timely fashion. We employ VPNs and MFA to provide secure access for our employees.
	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.	Our employee handbook defines expected employee behavior. Job descriptions outline roles and responsibilities. Our quality management system helps to assess and manage risk, ensuring our products are secure and compliant from design to delivery. Our ISO 13485 certification and annual SOC 2 Type 2 audits are instrumental in helping to ensure these policies are followed.
	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.	Our ISO 13485 quality management system has policies and procedures for managing and monitoring the organization's regulatory, legal, risk, and operational requirements. The policy is distributed to applicable employees, and those that have participatory roles are trained on their responsibilities regarding these policies.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ImPACT Applications has controls, procedures and policies in place to reduce and mitigate as much as possible any cybersecurity risk to organizational operations, data, assets, and individuals, including but not limited to secure development practices, network and internet boundary protections, and server protections.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	ImPACT Applications has a comprehensive risk management strategy that is part of our overall quality management system.
	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	ImPACT Applications has implemented a vendor evaluation and purchasing process to vet vendors and their products prior to purchase, ensuring they meet the designated criteria for their function.

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
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.	ImPACT Applications follows a Joiners and Leavers process that requires approval for account creation and prompt termination of access that is no longer necessary. This process is audited as part of our annual SOC 2 Type 2 audit.
	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.	ImPACT Applications has an employee training program in place and routinely assigns training exercises to employees on an as-needed basis. All employees receive a base-level of training when their employment begins, and additional items are added depending on job function and industry changes.
	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.	ImPACT Applications ensures all sensitive PII and PHI data are handled appropriately, stored in secure locations, and encrypted in transit and while at rest in our application database.
	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.	ImPACT Applications has a comprehensive set of IT policies and procedures, reviewed and approved by management that are followed and audited as part of our annual SOC 2 Type 2 audit.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	ImPACT Applications' IT policies and procedures contain sections addressing maintenance and patching of our systems.
	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.	ImPACT Applications periodically reviews all firewall rules associated with our application environments to ensure they are appropriate for our application needs. Any changes to the firewall rule set need to be reviewed and approved by management prior to being implemented.
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	All servers run HIDS software to monitor for any intrusion attempts and are configured to notify ImPACT Applications system administrators immediately if any anomalies are detected.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	ImPACT Applications monitors all servers with standard server & resource monitoring software to ensure they are operating properly. Additionally, we perform quarterly vulnerability scans and annual application security scans to check for and resolve any vulnerabilities found.

Function	Category	Contractor Response
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	HIDS and WAF configurations are reviewed periodically to ensure proper configuration and notification is in place.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	ImPACT Applications has a series of policies and procedures in place in the event a security event occurs. This policy includes information about notification requirements and time periods, investigation, and remediation.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	ImPACT Applications has a defined breach notification procedure that defines the tasks to complete, who to involve, when notifications are to go out and what they should contain.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	ImPACT Applications procedures include analysis phases to ensure an incident is sufficiently investigated to ensure the root problem is identified and corrected.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	ImPACT Applications will work to contain and limit the impact of any security event as quickly as possible, while preserving any information that would be helpful in investigating the root cause of the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	ImPACT Applications will take appropriate actions to mitigate or correct any issues that resulted in the origination of the incident to prevent any reoccurrence in the future.
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.	ImPACT Applications has a disaster recovery policy in place, tests the procedure annually, and ensures any required changes to the policy are made as needed.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	As part of our disaster recovery testing process, any lessons learned are incorporated into the policy so that it is continuously improved and accurate for current systems/applications.
	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).	ImPACT Applications has direct lines of communication with critical service providers, monitors communications and status pages for providers, alert messages and notifications from critical vendors. We subscribe to notification lists for services, software vendors and other service providers so that we can be aware of any service interruptions that may affect our services and customers.