EXHIBIT B – Education Law 2-d Rider and Parents' Bill of Rights

DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY
AND SUPPLEMENTAL INFORMATION ABOUT THE MLSA

1. Purpose

a) This Exhibit supplements and is fully incorporated into the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Nassau BOCES Parents' Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Nassau BOCES website.

b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. Definitions

Any capitalized term used but not defined within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

a) "Breach" is defined in Section 2-d and Part 121.

b) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

c) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

d) "Protected Data" means Student Data and/or Teacher or Principal Data processed by Vendor in the course of providing Vendor's Product or Services. Protected Data does not include information that has been anonymized or de-identified, anonymous usage data regarding a student's use of Vendor's services, or Public Content (as defined in Vendor's Terms of Service).

e) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a BOCES, and as a resultis licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Customer (Nassau BOCES) or any another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations and includes Nassau Participating Organizations and Licensees.

f) "Services" include Hudl products and services, including software and hardware, for use by sports teams for coaching, performance analysis, sport analysis, public game livestreaming, public game event ticketing, recruiting facilitation and athlete promotion, as described in the Agreement. The Services do not include any Hudl products and services used by fans of sports teams and fans, viewers and attendees of athletic and other events.

g) "Unauthorized Disclosure" or "Unauthorized Release" are defined in Section 2-d andPart 121.

h) For purposes of clarity, the definitions of "Student Data," "personally identifiable information" and "Protected Data" (1) do not include (a) video of or statistics or data related to publicly performed sporting events, or (b) public profile data; (2) relate only to data or information gathered or provided through or with respect to the Services; and (3) do not include any data or information provided to, gathered by or received by Vendor with respect to an individual's direct relationship with Vendor including where the individual is interacting with Vendor's fan experience.

i) "Vendor's Terms of Service" means the Organization Terms.

3. Confidentiality of Protected Data

a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with the MLSA, applicable federal and state law (including but not limited to Section2-d) and the Nassau BOCES policy on data security and privacy. Vendor acknowledges that Nassau BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, but that adoption may not occur until a date subsequent to the effective date of the MLSA. Nassau BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption, and Vendor and Nassau BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d. If Vendor determines it cannot comply with such policy, it may terminate the MLSA without liability or refund of fees.

c) Prior to any use of the Services, Participating Educational Agency shall, or shall cause public or private schools or school districts or Boards of Cooperative Education Services that purchase Services from Vendor through the MLSA ("Affiliated Schools") to, obtain written consent ("Consents") from each student's parent/legal guardian (or the eligible student directly) authorizing Vendor to (a) make public, share and disclose (i) video of and statistics and data related to publicly performed sporting events and (ii) public profile data for each student on the Services; and (b) share and disclose a student's profile data to verified recruiters, provided such disclosure or provision of profile data under (b) is consistent with the student's profile settings. Participating Educational Agency warrants that it will, or it will cause its Affiliated Schools to, have obtained all Consents before using the Services. Participating Educational Agency warrants that it will, or it will cause its Affiliated Schools to, keep all Consents on file and provide them to the Vendor upon request.

d) Vendor understands that any unauthorized disclosure, publication and/or communication of such Protected Data shall be considered a breach of the MLSA, excluding (1) disclosures permitted by the MLSA, Vendor's Terms of Service or as directed by the Participating Educational Agency; (2) disclosures of aggregate summaries of de-identified data; (3) disclosures to non-employee sub processors; or (4) disclosure or provision of a student athlete's profile data to verified recruiters, provided such disclosure is consistent with the student athlete's profile settings. Nothing in this Exhibit shall be interpreted to prohibit the disclosure or provision of a student athlete's profile data to verified recruiters, provided such disclosure or provision of profile data is consistent with the student athlete's profile settings.

4. Data Security and Privacy Plan

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Nassau BOCES Parents' Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

(a) In order to implement all applicable state, federal and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Nassau BOCES data security and privacy policy, Vendor states the following:

> *Hudl's information security program is modeled after the International Standards Organization (ISO) 27001 standard and designed to protect against the accidental or unauthorized damage, loss, or access of any Student or Participating Educational Agency/BOCES Data.*
>
> *Hudl's information security policy and data protection policy detail Hudl's approach to keeping data safe, private, and under control. These internal documents are reviewed quarterly, made available on Hudl's intranet, and used*

within internal awareness training. Hudl's privacy policy can be found at www.hudl.com/privacy and Hudl's security policy at www.hudl.com/security.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA:

Administrative:

Policies, standards, and procedures related to the classification, handling, retention, and destruction of data have been implemented and maintained. Hudl classifies all Student and Participating Educational Agency/BOCES Data at its highest level of data classification.

Hudl follows the principle of least privilege and system owners maintain and periodically review documentation regarding the privileges assigned to users, groups, and administrators.

Hudl provides security awareness training upon hire and at least annually. Attendance and completion are tracked through the Learning Management System (LMS). Hudl also performs background screening, testing, and reference checking as part of the hiring and onboarding process. All personnel, including third parties when applicable, are subject to confidentiality agreements.

Incident response and disaster recovery plans are maintained and tested to minimize the impact of potential threats to business operations.

Technical:

Hudl employs a defense-in-depth, zero-trust aligned strategy for network security including the use of host-based and web application firewalls, segregation of development, test, and production environments, and access control lists/security groups between Virtual Private Clouds (VPCs). Amazon Web Services (AWS) provides Distributed Denial-of-Service (DDoS) protection that ensures the uptime and availability of resources.

Hudl encrypts all Student and Participating Educational Agency/BOCES Data transferred over public networks following industry standard best practices. All Student and Participating Educational Agency/BOCES Data at rest within AWS environments is encrypted following industry standard best practices.

The software development life cycle includes several functional, non-functional and security testing requirements. Secure software development standards exist to guide and mature capabilities spanning threat modeling, third *party library risks, OWASP concerns, more formalized static/dynamic code testing and developer training. Change management and tracking is tied to role-based access and repositories are monitored.*

Hudl uses industry standard techniques designed to restrict access to and prevent unauthorized use of its systems. The use of individual user accounts is required to maintain the integrity of audit trails and access to resources is subject to the role of an employee. Password complexity and minimum key lengths are enforced for all identities. Multi-factor authentication is leveraged for employee access to all systems where supported.

Hudl continuously monitors its systems as well as the underlying infrastructure for suspicious activity. All systems generate security and operational logs, which are forwarded to the centralized logging system and monitored for anomalous activity that generates alerts for further investigation.

Physical:

Hudl is headquartered in the Haymarket District of Lincoln, Nebraska, with additional offices in Omaha, Nebraska; Boston, Massachusetts; London, United Kingdom; Sydney, Australia; Almeria, Spain; Den Bosch, Netherlands; Lexington, KY; Chiavari, Italy; Pune, India and Mumbai, India. Office locations are secured 24 hours a day, 365 days a year, with access solutions that restrict onsite and specific room access to personnel authorized based on their job function. Access is logged and available to support incident investigation if required, including staffed reception desks and video surveillance.

Hudl services and data are powered by AWS. Data is primarily stored in AWS's US-East (North Virginia) "us-east-1" region. Videos are stored within Amazon regions close to the uploading origin. While most of Hudl's infrastructure is located in the United States of America, there are AWS locations utilized inside the E.U., as well as other Third Countries protected by US approved Standard Contract Clauses. Amazon restricts physical access to people who need to be at a certain location at any time. Employees and vendors who have a need to be present at a data center must first apply for access and provide a valid business justification. The request is reviewed by designated personnel, including an area access manager. If access is granted, it is revoked once necessary work is completed.

(c) Vendor will comply with all obligations required by applicable law, set forth in the Nassau BOCES "Supplemental Information about the MLSA" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows:

> *Training is provided to new hires initially and on an ongoing basis on the confidentiality of customer and other sensitive information.*
>
> *Hudl has an internal tool that allows employees to encrypt sensitive messages sent between employees at Hudl. Employees have password-protected laptops.*

(e) Vendor *[check one]* X will _will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees or other authorized agents to enter into written agreements whereby subcontractors agree to secure and protect Protected Data in a manner consistent with the terms of the MLSA.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data in Vendor's possession, including identify Breaches and Unauthorized Disclosures, and Vendor will provide prompt notification of any confirmed Breaches or Unauthorized Disclosures of Protected Data in accordance with this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the reasonable return, transition, deletion and/or destruction of Protected Data upon Participating Educational Agencies' request, as more fully described in the Nassau BOCES "Supplemental Information about the MLSA," below.

5. Additional Statutory and Regulatory Obligations

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations may be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to Protected Data to be used only for the Services, by those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA) or by whom access is necessary for the Services.

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations, such as the Services, under the MLSA or Vendor's Terms of Service.

(c) Not use Student Data for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement and Vendor's Terms of Services.

(d) Not disclose any personally identifiable information to any other party, except as permitted under the Organization Terms and to carry out Vendor's obligations under the MLSA, unless:

(i) the parent or eligible student has provided prior written Consent; or

(ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(iii) the disclosure is permitted by Vendor's Terms of Service, the MLSA or this Data Sharing and Confidentiality Agreement; or

(iv) the Participating Educational Agency has directed such disclosure; or

(v) the disclosure is of aggregate summaries of de-identified data.

(e) Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in BOCES "Supplemental Information about the MLSA," below.

(g) Provide notification to Nassau BOCES (and Participating Educational Agencies, to the extent required by applicable law, and in accordance with this Data Sharing and Confidentiality Agreement) of any confirmed Breach of security resulting in an Unauthorized Release of Protected Data in Vendor's possession by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Where required by law, reimburse Nassau BOCES, another BOCES or a Participating School District for the required cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a Breach of Unauthorized Release of Protected Data attributed to Vendor or its subcontractors or assignees, only to the extent that such actions are not already performed by Vendor as part of its security breach response process.

6. Notification of Breach and Unauthorized Release

(a) Vendor shall promptly notify Nassau BOCES of any Breach or Unauthorized Release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has confirmed the Breach or Unauthorized Release.

(b) Vendor will cooperate with Nassau BOCES and provide as much information as possible directly to the General Counsel or designee about the Breach or Unauthorized Release, including but not limited to, to the extent known by Vendor, a description of the incident, the date of the incident (or an estimated date of the incident, or the date range), a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(c) Vendor acknowledges that upon notification from Vendor of a Breach or Unauthorized Release of Student Data, Nassau BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Nassau BOCES, Vendor will promptly inform General Counsel or designees.

(d) Vendor will consult directly with General Counsel or designees prior to providing any further notice of the Breach or Unauthorized Release (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

7. Vendor shall indemnify and hold Customer and each Licensee harmless from any third-party claims to the extent arising from Vendor's Breach or Unauthorized Disclosure or Unauthorized Release of Protected Data in Vendor's or its sub processor's possession resulting directly from Vendor or its sub processor's failure to comply with Vendor's Data Security and Privacy Plan in Section 4 of this Exhibit.

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

BY THE VENDOR:

By: ______________________

Title: Sales Manager

Date: 6/3/2024