

EXHIBIT C – 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 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 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 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 result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes BOCES or another BOCES that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.
- 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 and Part 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.

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 Section 2-d) and BOCES policy on data security and privacy. Vendor acknowledges that 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. BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption, and Vendor and 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 Third-party Contractor through the Agreement ("Affiliated Schools") to, obtain written consent ("Consents") from each student's parent/legal guardian 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 subprocessors, 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 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 BOCES data security and privacy policy, Vendor will:

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 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] 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 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 Org 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 student 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 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 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 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 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, 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 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.

PARENTS’ BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

BY THE VENDOR:

By:  _____

Title: Sales Manager

Date: 6/26/2024

SUPPLEMENTAL INFORMATION

Exclusive Purpose for which Protected Data will be Used:

Hudl will use Protected Data exclusively for the Services and as specified in this MLSA and Vendor’s Terms of Service.

Oversight of Subcontractors: Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these Agreements by entering into written Agreements whereby employees and subcontractors agree to secure and protect student data in a manner consistent with the terms of the Agreement.

Duration of MLSA and Protected Data Upon Expiration:

The period of this Data Sharing Confidentiality Request and Parents Bill of Rights will coincide with the term of the MLSA. Upon request, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors. Upon request, Vendor and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, that they are unable to access on their own through the Services, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Vendor will provide a list of the locations where Student Data is stored upon request. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

Encryption of Protected Data: Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

EXHIBIT D – BOCES Sign-on Form

AGREEMENT TO TERMS

Agile Sports Technologies, Inc. (“Vendor”) and Ulster BOCES (“Customer”) entered into the Master License and Service Agreement effective July 1, 2024 (the “MLSA”) under which Vendor has agreed to provide and Customer agrees to pay for certain Products to Customer and/or Customer’s authorized participating school districts and/or other educational institutions that elect to receive the Products (“Participants”). The Participant identified below desires to participate in the Agreement. This Agreement to Terms (“Participant Agreement”) demonstrates Participant’s intent to be bound by the terms and conditions of the MLSA.

Customer responds to program requests and initiatives from the New York State Education Department, and/or Participants and determines educational needs that would be most efficiently and cost effectively met on a regional, cooperative basis (the “Program”). Under the Program, Customer will pay for eligible Participants to utilize Vendor’s Licensed Products for its eligible students. Participants must follow Customer’s procedures to sign up and pay for the Products.

Pursuant to Paragraph 1 of the MLSA, Vendor has granted Customer and its authorized Participants the right to use certain Licensed Products in accordance with the terms of the Master Agreement. Participant identified below has elected to participate in the Program.

Accordingly, Participant agrees as follows:

1. The capitalized terms in this Participant Agreement shall refer to and have the same meaning as the capitalized terms in the MLSA.
2. That Participant is hereby bound by the terms and conditions of the MLSA, including, but not limited to, the Hudl Organization Terms of Service (“Organization Terms”) and all other applicable Exhibits, and this Participant Agreement, and shall participate in the MLSA as a Participant. The Participant shall be deemed an “Organization” for purposes of the Organization Terms.
3. Participant is responsible for complying with the requirements of New York Education Law Section 2-d and its implementing regulations, Part 121 of the Commissioner’s Regulations, as such are applicable to the MLSA, including but not limited to receiving, investigating, and responding to parent complaints.
4. That the Products available to Customer and Participant, as set forth in the MLSA, are limited to the Licensed Products ordered by Customer and Participant.
5. Subject to the terms of the MLSA, Participant agrees to receive the Products selected by it and as set forth in the MLSA. Participant shall be solely responsible for any and all Products received by it through the MLSA.

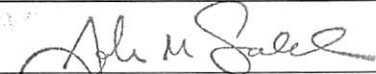
Participating School District Name	Street	City, State & Zip			Phone
School/District Name	Shipping Street	City	State	Zip/Postal Code	Account Phone
Site Contact Name		Site Contact Title	Site Contact Email		

6. This Participant Agreement shall become effective on the date the Participant signs the Participant Agreement and shall be coterminous with the Master Agreement. Any changes to the Master Agreement, the Licensed Products, the descriptions of Products and/or pricing agreed to between Vendor and Customer shall automatically be included in this Participant Agreement without the requirement for an amendment.
7. Participant agrees to comply with all Vendor-required information and deadlines in order to participate in selected Products and Services.
8. Participant may terminate this Participant Agreement with cause upon thirty (30) days written notice to the other two parties. In the event that this Participant Agreement is terminated, the Master Agreement shall remain in full force and effect and shall be enforceable in accordance with its terms. If the Master Agreement is terminated/cancelled, then this Participant Agreement shall be immediately terminated/cancelled. If Participant terminates this Participant Agreement, the parties remain liable for payment of all Fees owed for the current subscription term and will not be entitled to a credit or refund.
9. Participant represents and warrants (a) that it has the requisite authority to execute this Participant Agreement; and (b) that the individual(s) signing the Participant Agreement on behalf of such party is (are) authorized to do so. Participant may and hereby does bind itself to the terms and conditions of the Master Agreement, including without limitation, the Org Terms and all applicable schedules and addenda.

Execution of this Participant Agreement shall have no effect on the enforceability of the Master Agreement in accordance with its terms.

PARTICIPANT

(District): _____

Signature: 

Printed Name: Jonah Schenker

Title: District Superintendent

Date: 7/11/2024

EXHIBIT E – Recruit Participation

Included at no additional cost in every Hudl subscription is an expanded athlete recruiting profile. Athletes must opt in to recruiting and allow their Hudl profile to be viewed by registered recruiters (verified collegiate athletic recruiters and coaches). Additionally, via the Hudl platform, team admins control whether team highlights and athlete profiles are publicly viewable or if they may be viewable only by team members. Such use of the Hudl platform is governed by the Hudl Organization Terms of Service (found attached as Exhibit A).

EXHIBIT F – Training

Explanation of Training

Initial Training for Athletic Department Packages

Kick-Off Call with Customer Success Manager

- Determine training schedule
- Identify key areas to be included in training session

Online Customer Success Training (CST)

- 30-min session
- Customer Success Manager will conduct a District-wide training for coaches
- Ad-hock trainings applicable when required for success

Further Training and Resources

Hudl Academy

- Self-paced learning resources for coaches
- hudl.com/academy

Hudl Support Expert Chats

- Schedule one-on-one trainings with a Hudl Support team member
- calendly.com/hudl-support/

Hudl Support Webpage

- Search a wide variety of FAQ and support tutorials.
- hudl.com/support

Services

The “Services” generally 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 MLSA. 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.

IRAN DIVESTMENT ACT OF 2012 CERTIFICATION

As a result of the Iran Divestment Act of 2012 (Act), Chapter 1 of the 2012 Laws of New York, added new provisions to the State Finance Law (SFL), §165-a and General Municipal Law (GML) §103-g effective April 12, 2012. Under the Act, the Commissioner of the Office of General Services (OGS) will be developing a list (prohibited entities list) of "persons" who are engaged in "investment activities in Iran" (both are defined terms in the law). Pursuant to SFL § 165-a(3)(b) and GML §103-g, the initial list is expected to be issued no later than 120 days after the Act's effective date, at which time it will be posted on the OGS website.

By submitting a response to this solicitation or by assuming the responsibility of a Contract awarded hereunder, Vendor (or any assignee) certifies that once the prohibited entities list is posted on the OGS website, it will not utilize on such Contract any subcontractor that is identified on the prohibited entities list.

Additionally, Vendor is advised that once the list is posted on the OGS website, any Vendor seeking to enter into, renew or extend a Contract or assume the responsibility of a Contract awarded in response to the solicitation, must certify at the time the Contract is bid upon or a proposal submitted, or the contract is renewed, extended or assigned that it is not included on the prohibited entities list.

During the term of the Contract, should BOCES receive information that a person is in violation of the above-referenced certification, BOCES will offer the person an opportunity to respond. If the person fails to demonstrate that it has ceased its engagement in the investment which is in violation of the Act within 90 days after the determination of such violation, then BOCES shall take such action as may be appropriate including, but not limited to, imposing sanctions, seeking compliance, recovering damages, or declaring the Vendor in default.

BOCES reserves the right to reject any bid, proposal or request for assignment for an entity that appears on the prohibited entities list prior to the award of a contract, and to pursue a responsibility review with respect to any entity that is awarded a contract and appears on the prohibited entities list after contract award.

Signature:  _____

Print Name: **Tyler Kvasnicka** _____

Title: **Sales Manager** _____

Company Name: **Agile Sports Technologies Inc dba. Hudl** _____

Date: **6/26/2024** _____