CALIFORNIA STUDENT DATA PRIVACY AGREEMENT
Version 2.0 (September 26, 2018)

Irvine Unified School District

and

Agile Sports Technologies, Inc., dba Hudl

November 18, 2020

This California Student Data Privacy Agreement ("DPA") is entered into by and between the school district, Irvine Valley Unified School District (hereinafter referred to as "LEA") and Agile Sports Technologies, Inc., dba Hudl (hereinafter referred to as "Provider") on November 18, 2020. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated [November 18, 2020] ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive or create and the LEA may provide documents or data that are covered by several federal statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g (34 CFR Part 99), Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services are also subject to California state student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act ("SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, for the purposes of this DPA, Provider is a school official with legitimate educational interests in accessing educational records pursuant to the Service Agreement; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms" (Exhibit "E"), agree to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1 **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from LEA pursuant to the Service Agreement, including compliance with all applicable statutes, including the FERPA, PPRA, COPPA, SOPIPA, AB 1584, and other applicable California State laws, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. With respect to the use and maintenance of Student Data, Provider shall be under the direct control and supervision of the LEA.

2 **Nature of Services Provided**. The Provider has agreed to provide the digital educational products and services described below and as may be further outlined in Exhibit "A" hereto:

The Hudl software, app and services, which together comprise an online tool to review game footage, improve team play and facilitate recruiting, as described in its terms of use, end user license agreement and privacy policy.

3 **Student Data to Be Provided**. The Parties shall indicate the categories of student data to be provided in the Schedule of Data, attached hereto as Exhibit "B".

4 **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1 **Student Data Property of LEA**. All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this Agreement in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of Student Data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below. Notwithstanding the foregoing, the LEA grants Provider a non-exclusive, royalty-free right to use Student Data to (a) provide the Services, (b) permit recruiters confirmed by Provider's affiliate, Haymarket Recruiting, LLC, to access the Student Data for recruiting purposes only if the Provider receives parental consent for the relevant students to share with recruiters, and (c) to the extent the LEA enables public sharing of highlight videos ("Highlights") from within Provider's platform, to (1) use Highlights to provide the Service's community features to users and to other third parties during the Term, and (2) to reproduce, transmit, display, exhibit, distribute, index, comment on, modify, create derivative works based upon (including inserting advertising therein), perform and otherwise use the Highlights, in whole or in part, in perpetuity in all media formats and channels now known or hereafter devised (including on Provider's websites, third party websites, cable networks and stations, broadband and wireless platforms, products and services) for any and all purposes, including entertainment, news, advertising, promotional, marketing, publicity, trade or commercial purposes, all without further notice to, or permission from the LEA, with or without attribution and without any royalty or payment obligations, which rights in this subsection (c) shall survive any termination or expiration of this DPA.

2 **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Student Data in the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. To the extent particular Student Data is not available for the LEA to view or correct from within Provider's platform, the Provider shall respond in a timely manner (and no later than 45 days from the date of the request) to the LEA's request for Student Data in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of

Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3 **Separate Account**. If pupil generated content is stored or maintained by the Provider as part of the Services described in Exhibit "A", Provider shall, at the request of the LEA, transfer said pupil generated content to a separate student account upon termination of the Service Agreement; provided, however, such transfer shall only apply to pupil generated content that is severable from the Service.

4 **Third Party Request**. Should a Third Party, including law enforcement, and government entities, contact Provider with a non-legally compelled request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party, unless legally prohibited and except for the disclosure described in Article II.1(b) and/or (c), and/or unless a parent or legal guardian has provided consent to the LEA or the Provider for Student Data to be disclosed to a Third Party.

5 **Subprocessors**. Notwithstanding any language to the contrary in this DPA, Provider may utilize Subprocessors in providing the Services; provided that Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in manner consistent with the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Laws**. LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, SOPIPA, AB 1584, and all other California privacy statutes.

2. **Annual Notification of Rights**. If the LEA has a policy of disclosing education records under FERPA (4 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

4. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. In its provision of Services to the LEA, the Provider shall comply with all California and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, SOPIPA, AB 1584 and all other California privacy statutes.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above. Except for the disclosure described in Article II.1(b) and/or (c), and/or as expressly consented by the applicable user, Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA, unless it fits into the de-identified information exception in Article IV, Section 4, or there is a court order or lawfully issued subpoena for the information.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement.

4. **No Disclosure**. De-identified information may be used by the Provider for the purposes of development, research, and improvement of educational sites, services, or applications, as any other member of the public or party would be able to use de- identified data pursuant to 34 CFR 99.31(b). Provider agrees not to attempt to re-identify de-identified Student Data and not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Provider shall not copy, reproduce or transmit any data obtained under the Service Agreement and/or any portion thereof, except as necessary to fulfill the Service Agreement.

5. **Disposition of Data**. Upon written request, Provider shall dispose or delete all Student Data obtained under the Service Agreement within sixty (60) days of a request by LEA. Nothing in the DPA authorizes Provider to maintain personally identifiable data obtained under any other writing beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Student Data; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable by human or digital means. Nothing in the Service Agreement authorizes Provider to maintain Student Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Provider shall provide written notification to LEA when the Student Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the Service Agreement.

6. **Advertising Prohibition.** Provider shall not (a) use Student Data for Targeted Advertising; or (b) provide or match Student Data to inform, influence, or enable marketing or advertising efforts on Provider's platform; or (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client. This prohibition does not prohibit Provider from using Student Data as necessary to provide the Service to Client.

ARTICLE V: DATA PROVISIONS

1. Data Security. The Provider agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in Exhibit "F" hereto. These measures shall include, but are not limited to:

   a. **Passwords and Employee Access.** Provider shall secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by the applicable standards, as set forth in Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. Employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall be subject to criminal background checks in compliance with state and local ordinances.

   b. **Destruction of Data.** Provider shall destroy or delete all Student Data obtained under the Service Agreement upon request by the LEA or transfer said data to LEA or LEA's designee, according to a schedule and procedure identified in Article IV, section 5, above.as the parties may reasonable agree.

   c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure digital environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

   d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

   e. **Security Technology.** When the service is accessed using a supported web browser, Provider shall employ industry standard measures to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is updated according to industry standards.

   f. **Security Coordinator.** If different from the designated representative identified in Article VII, section 5, Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement.

   g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

   h. **Periodic Risk Assessment.** Provider further acknowledges and agrees to conduct digital and physical periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

2. **Data Breach**. In the event that unencrypted Student Data is accessed or obtained by an unauthorized individual, in accordance with applicable law, Provider agrees to notify the LEA within a reasonable amount of time (and not exceeding fifteen (15)) days following Provider's internal confirmation of a breach that impacts the LEA's unencrypted information, unless prohibited from doing so by law enforcement or a regulatory authority, in which case Provider will provide notice promptly in accordance with the circumstances. Unless the applicable law of an impacted user's state of resident provides otherwise, Provider shall follow the following process:

   a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

   b. Provider agrees to adhere to all applicable state and federal requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

   c. Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to make employees available at reasonable times to discuss the written incident plan.

   d. At the request of the District, Provider shall provide reasonable assistance to the District notify the affected parent, legal guardian or eligible pupil of the unauthorized access.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

   The LEA may terminate this DPA and the Service Agreement if the Provider materially breaches any terms of this DPA.

3. **Priority of Agreements**. This DPA shall govern the treatment of student data in order to comply with privacy protections, including those found in FERPA, and all privacy statutes identified in this DPA. In the event there is conflict between the DPA and the Service Agreement, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Notice**. All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives below.

   The designated representative for the Provider for this Agreement is:

   Legal
   Hudl
   600 P Street
   Suite 400
   Lincoln, NE 68508
   legal@hudl.com

   The designated representative for the LEA for this Agreement is:

   Name: Michelle Bennett
   Title: IT Contracts Specialist
   Address: 5050 Barranca Parkway
   Irvine, CA 92604
   Email MichelleBennett@iusd.org

Entire Agreement. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES.

7. **Authority**. Provider represents that it is authorized to bind to the terms of this Agreement, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof, or may own, lease or control equipment or

facilities of any kind where the Student Data and portion thereof stored, maintained or used in any way.

8. Waiver. No delay or omission of the LEA to exercise any right hereunder shall be construed as a waiver of any such right and the LEA reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

9. Electronic Signature: The parties understand and agree that they have the right to execute this Agreement through paper or through electronic signature technology, which is in compliance with California and Federal law governing electronic signatures. The parties agree that to the extent they sign electronically, their electronic signature is the legally binding equivalent to their handwritten signature. Whenever they execute an electronic signature, it has the same validity and meaning as their handwritten signature. They will not, at any time in the future, repudiate the meaning of my electronic signature or claim that their electronic signature is not legally binding. They agree not to object to the admissibility of this Agreement as an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the grounds that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

   Each party will immediately request that their electronic signature be revoked in writing if they discover or suspect that it has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way. They understand that they may also request revocation at any time of their electronic signature for any other reason in writing.

   If either party would like a paper copy of this Agreement, they may request a copy from the other party.

10. Multiple Counterparts: This Agreement may be executed in any number of identical counterparts. If so executed, each of such counterparts shall constitute this Agreement. In proving this Agreement, it shall not be necessary to produce or account for more than one such counterpart. Execution and delivery of this Agreement by .pdf or other electronic format shall constitute valid execution and delivery and shall be effective for all purposes (it being agreed that PDF email shall have the same force and effect as an original signature for all purposes).

ARTICLE VII- GENERAL OFFER OF TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached hereto as Exhibit "E"), be bound by the terms of this to any other school district who signs the acceptance in said Exhibit.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this California Student Data Privacy Agreement as of the last day noted below.

Local Education Agency: Irvine Unified School District

____ Date: November 18, 2020

Printed Name: John Fogarty Title/Position: Asst. Supt. Business Services

IUSD Board Approved 11|17|2020

AGILE SPORTS TECHNOLOGIES, INC., DBA HUDL

____ Date: 10/28/20

Printed Name: BRETT SHAMBLIN Title/Position: DIRECTOR OF SALES

EXHIBIT "A"

DESCRIPTION OF SERVICES

Hudl, an online tool to review game footage, improve team play and facilitate college recruitment of students, as described in its terms of use, end user license agreement and privacy policy.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, use of cookies etc.	X
	Other application technology meta data. Please specify:	
Application Use Statistics	Meta data on user interaction with application	X
Assessment	Standardized test scores	
	Observation data	
	Other assessment data. Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	X
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	

Category of Data	Elements	Check if used by your system
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred, or primary language spoken by student)	
	Other demographic information. Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	X

	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/health data	
	Student disability information	
	Specialised education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information. Please specify:	
Student Name	First and/or Last	X
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	X
Transportation	Student bus assignment	

	Other enrollment information. Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone Number	
	State ID number	
Student Contact Information	Address	
	Email	X
	Phone	X
Student Survey Responses	Student responses to surveys or questionnaires	
Student In App Performance	Program/application performance (ex: typing program-student types 60 wpm, reading program- student reads below grade level)	
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:	

	Student pick up and/or drop off location		Other	Please list each additional data element used, stored, or collected by your application.	Video and statistics from athletic events
	Student bus card ID number				
	Other transportation data. Please specify:				

EXHIBIT "C"

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Provider removes or obscures any Personally Identifiable Information ("PII") from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

Educational Records: Educational Records are official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs. For purposes of this DPA, Educational Records are referred to as Student Data.

NIST: Draft National Institute of Standards and Technology ("NIST") Special Publication Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Student Data.

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the DPA the term "Provider" includes the term "Third Party".

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employee. For the purposes of this Agreement, Pupil Records shall be the same as Educational Records, Student Personal Information and Covered Information, all of which are deemed Student Data for the purposes of this Agreement.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to 34 CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to 34 CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

SOPIPA: Once passed, the requirements of SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information.

Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

SDPC (The Student Data Privacy Consortium): Refers to the national collaborative of schools, districts, regional, territories and state agencies, policy makers, trade organizations and marketplace providers addressing real-world, adaptable, and implementable solutions to growing data privacy concerns.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Irvine Unified School District directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider.

The terms of the Disposition are set forth below:

Extent of Disposition Disposition shall be:	Partial. The categories of data to be disposed of are as follows: Complete. Disposition extends to all categories of data.
Nature of Disposition Disposition shall be by:	Destruction or deletion of data. Transfer of data. The data shall be transferred as set forth in an attachment to this Directive. Following confirmation from LEA that data was successfully transferred, Provider shall destroy or delete all applicable data.
Timing of Disposition Data shall be disposed of by the following date:	As soon as commercially practicable By (Insert Date)

Authorized Representative of LEA Date

Verification of Disposition of Data Date by
Authorized Representative of Provider

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERM

1. Offer of Terms.

Provider offers the same privacy protections found in this DPA between it and the LEA to any other school district ("Subscribing LEA") who accepts this General Offer though its signature below. The Provider agrees that the information on the next page will be replaced throughout the Agreement with the information specific to the Subscribing LEA filled on the next page for the Subscribing LEA. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provide by LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products subject listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the LEA in the event of any withdrawal so that this information may be transmitted to the Subscribing LEAs.

AGILE SPORTS TECHNOLOGIES, INC., DBA HUDL

BY:______________________ Date: 10/28/20

Printed Name: Jordan Shamblin Title/Position: Director of Sales

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA's individual information is contained on the next page. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

BY:______________________ Date:______________________

Printed Name:______________________ Title/Position:______________________

SCHOOL DISTRICT NAME:______________________
DATE:______________________

DESIGNATED REPRESENTATIVE OF LEA:

Name ______________________
Title ______________________
Address ______________________
Telephone Number ______________________
Email ______________________

COUNTY OF LEA:______________________

EXHIBIT "F"

PROVIDER SECURITY

[ATTACHED]