

STANDARD STUDENT DATA PRIVACY AGREEMENT

OHIO

OH DPA, Modified Version 1.0

NORTH CENTRAL LOCAL SCHOOLS

and

AGILE SPORTS TECHNOLOGIES, INC., DBA HUDL

This Student Data Privacy Agreement (“**DPA**”) is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between: North Central Local Schools, located at 400 E Baubice St., Pioneer, Ohio 43554 (the “**Local Education Agency**” or “**LEA**”) and Agile Sports Technologies, Inc., dba Hudl, located at 600 P St., Ste 400, Lincoln, NE, 68508 (the “**Provider**”).

WHEREAS, the Provider is providing digital services to LEA, which plans to use such services for educational purposes.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. § 1232g (34 CFR Part 99); the Children’s Online Privacy Protection Act (“**COPPA**”) at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.
2. **Special Provisions. Check if Required**
 If checked, the Supplemental State Terms and attached hereto as **Exhibit “G”** are hereby incorporated by reference into this DPA in their entirety.
 If Checked, the Provider, has signed **Exhibit “E”** to the Standard Clauses, otherwise known as General Offer of Privacy Terms
3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.
4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.
5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”).
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: Greg Nelson, SVP, Competitive
Address: 600 P Street, Suite 400 Lincoln, NE 68508
Phone: 402-817-0060
Email: legal@hudl.com

The designated representative for the LEA for this DPA is:

Name: Travis A. Creek, Technology Director
Address: 400 E Babuice St. Pioneer, OH 43554
Phone: 419-737-2392 x 5298
Email: tcreek@northcentralschools.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

NORTH CENTRAL LOCAL SCHOOL


By: 
Travis Creek (Oct 28, 2024 16:34 EDT)

Date: 10/28/2024

Printed Name: Travis A. Creek

Title/Position: Technology Director

AGILE SPORTS TECHNOLOGIES, INC., DBA HUDL

By: 
Derek Hansen (Oct 28, 2024 16:46 EDT)

Date: 10/28/2024

Printed Name: Derek Hansen

Title/Position: Sr. Manager, Competitive Sales

STANDARD CLAUSES

Version 1.0

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 including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider will act as a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data.
- 2. Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B"**.
- 3. 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 any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

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 DPA 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 will act as a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above. To the extent particular Student Data is not available for the LEA to access on its own from within Provider's platform, the Provider will use reasonable efforts to cooperate and provide such Student Data within Provider's possession within the earlier of, after LEA's reasonable written request, forty-five (45) days or the time frame required under applicable state law for an LEA to respond. Notwithstanding the foregoing, the LEA grants Provider a non-exclusive, royalty-free right to use Student Data to (a) provide the Services, (b) where the LEA uses such features of the Services, to share practice video or game video, including related information and statistics, with another user of the Provider's platform (as designated by the LEA), (c) permit verified recruiters to access the Student Data, including an athlete's profile information, for recruiting purposes provided the disclosure or provision of such Student Data is consistent with the athlete's privacy settings (provided that the LEA did not disable recruiting for such athlete through the Provider's platform), (d) to publicly share an athlete profile page on the Platform, unless the LEA disables this via the Provider's platform, and (e) 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 (e) shall survive any termination or expiration of this DPA.

2. **Parent Access.** To the extent required by law, the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Educational Records and/or Student Data, correct erroneous information, and create procedures for the transfer of Student-Generated Content to a personal account, consistent with the functionality of the Services. The Provider shall use reasonable efforts to respond within, the earlier of, (x) 45 days or (y) the time frame required under state law for an LEA to respond, to any reasonable written request by LEA for Student Data in the possession of the Provider to view or correct as necessary where LEA is not able to do so on its own through the Services. In the event that a parent of a student or other individual contacts the Provider to review any of the 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 Student Data.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities (“Requesting Party(ies)”) contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request or unless legally prohibited.
5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Educational Records and/or Student Data under FERPA (34 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 Student 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.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A, as stated in this DPA, for the disclosures described in Article II, Section 1(b), (c), (d) or (e) of this DPA, as requested in writing by the LEA, and/or as otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Except for the disclosures described in Article II, Section 1(b), (c), (d) or (e) and/or unless expressly consented to by a parent or legal guardian, Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed by the LEA or this DPA or where otherwise permitted under applicable law. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified Data, Student Data disclosed pursuant to a court order, lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Except for the disclosures described in Article II, Section 1(b), (c), (d) or (e) and/or unless a parent or legal guardian has provided consent to the LEA or the Provider for Student Data to be disclosed, transferred, or shared with a third party, Provider will not sell Student Data to any third party. Nothing in this DPA shall be interpreted to prohibit the disclosure or provision of video or statistics or data related to publicly performed sporting events or public profile data as outlined in Article II, Section 1(b), (c), (d) or (e) to provide 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.
 5. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; (2) improvement, research and development of the Provider's sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors and Affiliates, Provider agrees not to transfer De-Identified Student Data to any party unless (1)(a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer.
6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of

Data” form, a copy of which is attached hereto as **Exhibit “D”**. If the LEA and Provider employ Exhibit “D,” no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit “D.”

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Services to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States.
2. **Audits.** No more than once each year of the term of this DPA and upon written request from the LEA, Provider will provide its security due diligence artifacts, including an updated security posture overview and HECVAT. Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of Provider and/or delivery of Services to students and/or LEA as required by applicable law.
3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit “F”**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “F”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seven (7) days of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after discovery of the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of Student Data that were or are reasonably believed to have been the subject of a breach.

- iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state 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.
- (3) 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 provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: 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 **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **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. Either party may terminate this DPA upon a material breach of this DPA by the other party.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between the SDPC Standard Clauses and the

Supplemental State Terms, the Supplemental State Terms will control. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute 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; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION OF THE STATE AND FEDERAL COURTS LOCATED IN MASSACHUSETTS FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event of a change of control of Provider where an unaffiliated third party (that is not a current or future affiliate or current shareholder, directly or indirectly, of Provider) acquires all or substantially all of the assets of Provider, Provider will provide written notice to LEA within a reasonable time period after such change of control, and LEA may terminate this DPA upon written notice within ninety (90) days of learning of such change in control if such change in control violates applicable law.
8. **Limitation of Liability.** TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL THE AGGREGATE LIABILITY OF EITHER PARTY (INCLUDING EITHER PARTY'S AFFILIATES AND PROVIDER'S SUPPLIERS), ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY LEA UNDER THE SERVICE AGREEMENT IN THE TWELVE MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT, TORT, OR ANY OTHER THEORY OF LIABILITY, BUT WILL NOT LIMIT EITHER PARTY'S PAYMENT OBLIGATIONS.
9. **Exclusion of Consequential and Related Damages.** IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, OR REVENUES, LOSS OF REPUTATION OR GOODWILL, OR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, ENHANCED, COVER, BUSINESS INTERRUPTION OR PUNITIVE DAMAGES,

WHETHER AN ACTION IS IN CONTRACT, TORT, OR ANY OTHER THEORY OF LIABILITY, EVEN IF A PARTY OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSSES OR DAMAGES OR IF A PARTY'S OR ITS AFFILIATES' REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE. THE FOREGOING LIMITATION WILL NOT APPLY TO THE EXTENT IT IS PROHIBITED BY APPLICABLE LAW.

- 10. Authority.** Each party represents that it is authorized to bind to the terms of this DPA, 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.
- 11. Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"
DESCRIPTION OF SERVICES

The 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 Service 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.

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	X
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	X
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	X
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	

Category of Data	Elements	Check if Used by Your System
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	X
	Email	X
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Provider/App assigned student ID number	
	Student app username	X
	Student app passwords	X
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)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
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:	

Category of Data	Elements	Check if Used by Your System
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: Photo, video, stats from athletic events	X
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	

EXHIBIT "C" DEFINITIONS

Affiliate: An affiliate means, in the case of either party, any other person or entity (a) controlling, (b) controlled by or (c) under common control with such party.

De-Identified Data and De-Identification: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such 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 clarity, the definition of "Educational Records" as used in this DPA (1) does not include (a) video of or statistics or data related to publicly performed sporting events, or (b) public profile data; (2) relates only to data or information gathered or provided through or with respect to the Services; and (3) does not include any data or information provided to, gathered by or received by Hudl with respect to an individual's direct relationship with Hudl including where the individual is interacting with Hudl's fan experience.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation. Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used by the Originating LEA for K-12 school purposes.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator".

Student Generated Content: The term "Student-Generated Content" means materials or content created by a student in the Services 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 student content.

School Official: For the purposes of this DPA 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 Student Data including Educational Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Educational Records.

Service Agreement: Refers to Order Form(s) executed between the LEA and Provider and Provider's Organization Terms of Service found at www.hudl.com/eula and any additional terms agreed to through the Services by the school admin in the Hudl account, as set in the account on the Services ("**Provider's Terms of Service**").

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, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or 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, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Educational Records for the purposes of this DPA, and for the purposes of applicable federal, state, and local 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. For purposes of clarity, the definitions of "Student Data" and "personally identifiable information (PII)" as used in this DPA (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 Hudl with respect to an individual's direct relationship with Hudl including where the individual is interacting with Hudl's fan experience.

Subprocessor: For the purposes of this DPA, 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 service, and who has access to Student Data.

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback or any advertising to a student when not logged into the Services.

Third Party: The term "Third Party" means a provider of digital software or services, including cloud-based services, for the digital storage, management, and retrieval of information.

EXHIBIT "D"
DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] 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:

1. Extent of Disposition

_____ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

[Insert categories of data here]

_____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

_____ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

4. Signature

Authorized Representative of LEA

Date

5. Verification of Disposition of Data

Authorized Representative of Company

Date

EXHIBIT "E"
GENERAL OFFER OF PRIVACY TERMS

Intentionally omitted.

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
X	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
X	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)**
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit <http://www.edspex.org> for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

**Provider’s security policies and standards are aligned with NIST SP 800-53 and ISO 27000/01.

EXHIBIT "G"

Ohio

WHEREAS, the documents and data transferred from LEAs and created by the Provider's Services may be subject to several state laws in Ohio. Specifically, those laws are O.R.C. §§ 3319.32-3319.327, O.R.C. §§ 1349.17-19, Rule 3301-51-04; and

WHEREAS, the Parties wish to enter into these supplemental terms to the DPA to ensure that the Services provided conform to the requirements of the privacy laws referred to above and to establish implementing procedures and duties;

WHEREAS, the Parties wish these terms to be hereby incorporated by reference into the DPA in their entirety for Ohio;

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

1. In Article IV, Section 2, replace "otherwise authorized," with "otherwise required."
2. In Article IV, Section 3, add: "The Provider will restrict unauthorized access by Provider's employees or contractors not providing services under the Service Agreement or DPA and its employees or contractors will only access Student Data as necessary to fulfill their official duties."
3. [intentionally omitted]
4. All employees of the Provider who will have direct contact with students shall pass criminal background checks.
5. In Article V, Section 1 Data Storage: Ohio does not require data to be stored within the United States.

With respect to Student Data, Hudl agrees to comply with all applicable student data protection laws of Ohio, including O.R.C. 3319.325-3319.327, in effect as of October 24, 2024.