

This Student Data Privacy Agreement (**DPA**) is entered into by and between:

THE BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY, a political subdivision of the Commonwealth of Kentucky, with its principal place of business at 3332 Newburg Road, Louisville, Kentucky 40218 (the “**Board**” or “**Jefferson County Public Schools**”) and

Hudl, Inc., a Corporation organized under the laws of Delaware with its principal place of business located at 600 P Street, Suite #400, Lincoln, NE 68508 (the “**Provider**”).

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

WHEREAS, the Provider and the Board 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 the Board 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, the Board and Provider agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement between the Parties and supersedes any and all agreements, representations, and negotiations, either oral or written, between the Parties before the effective date of this DPA. This DPA may not be amended or modified except in writing as provided below. This DPA is supplemented by the Board’s Procurement Regulations currently in effect (hereinafter “**Regulations**”) that are incorporated by reference into and made part of this DPA. In the event of a conflict between any provision of this DPA and the Regulations, the Regulations shall prevail. 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.
2. **Term.** This DPA shall be effective as of March 31, 2026 (the “**Effective Date**”) and shall continue for ~~three (3) years~~, one (1) year, terminating on March 10, 2027.
3. **Services.** The services to be provided by Provider to the Board pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”). Any compensation to be provided by the Board to Provider is also detailed in **Exhibit “A”** (the “**Compensation**”). Each party shall be responsible for their portion of costs that may result from data sharing. Examples of potential costs to the Board are costs associated with the compiling of Student Data requested under this DPA and costs associated with the electronic delivery of Student DATA to Provider.
4. **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

shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the Board. Provider shall be under the direct control and supervision of the Board, with respect to its use of Student Data. This DPA is incorporated into and made part of the Service Agreement.

5. **Student Data to Be Provided.** In order to perform the Services described above, the Board shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
6. **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 the Board.** 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 Board. 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 Board. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the Board as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the Board 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 procedures for the transfer of Student-Generated Content to a personal account, consistent with the functionality of Services. The Provider shall use reasonable efforts to respond within 45 days to any reasonable written request by the Board for Student Data in the possession of the Provider to view or correct as necessary where the Board 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 Board, who will follow the necessary and proper procedures regarding the Student Data.
3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the Board, transfer, or provide a mechanism for the Board 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 Board in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Board 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.

- 6. Research and Program Evaluation.** For any project, involving data collection or research (e.g., program evaluation or monitoring activities), student or staff participation is voluntary. As a federally authorized Institutional Review Board (IRB), the Board complies with the federal definition for research, which includes sharing of Personally Identifiable Information (PII) for the purposes of answering a question or evaluating activities for effectiveness beyond standard educational or operational procedures. Thus, all data collection and research activities must be approved by the Board's IRB and shall not begin before approval is secured from the IRB. If Provider wishes to collect data specifically for program evaluation or research purposes, or if Provider wishes to use identifiable data for program evaluation or research purposes, Provider must apply for and obtain permission from the Board's IRB prior to beginning any research or evaluation related data collection.

ARTICLE III: DUTIES OF THE BOARD

- 1. Provide Data in Compliance with Applicable Laws.** The Board 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 Board has a policy of disclosing Educational Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), the Board 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.** The Board 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.** The Board shall notify Provider promptly of any known unauthorized access. The Board 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, including but not limited to, in each case to the extent applicable to the Provider's processing of Student Data under this Agreement, FERPA; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; 7 C.F.R. 245.6 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.
- 2. Data Custodian.** For the purposes of this DPA and ensuring Provider's compliance with the terms of this DPA and all application of state and federal law, Provider designated Cameron Calkins as the data custodian ("Data Custodian") of the Student Data. The Board will release all data and information under this DPA to Data Custodian. Data Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data requested and received pursuant to this DPA, including confirmation of the return or destruction of data as

described below. The Board may, upon request, review the records Provider is required to keep under this DPA.

3. **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"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA. Provider will not contact the students included in the Student Data sets without obtaining advance written authorization from the Board, except as provided in the Service Agreement.
4. **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.
5. **No Disclosure.** Except as permitted by the Service Agreement, 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 Board or this DPA or where otherwise permitted under applicable law. If Provider becomes legally compelled to disclose any Student Data (whether by judicial or administrative order, applicable law, rule, regulation, or otherwise), then Provider shall use all reasonable efforts to provide the Board with prior notice before disclosure where legally permissible so that the Board may seek a protective order or other appropriate remedy to present the disclosure or to ensure the Board's compliance with the confidentiality requirements of federal or state law. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, 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 as otherwise permitted by the Service Agreement, 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 described in the Service Agreement, or disclosure or provision of athlete's profile data to verified recruiters, provided such disclosure or provision of profile data is consistent with the athlete's privacy settings.
6. **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 Board or other governmental agencies in conducting research and other studies; and (2) improvement, research and development of the Provider's educational 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 the Board 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 Board who has provided prior written consent for such transfer or (2) Student Data has been sufficiently aggregated that it cannot be re-identified. Prior to publishing any document that names the Board explicitly or indirectly, the Provider shall obtain the Board's prior written approval.

7. **Disposition of Data.** Upon written request from the Board, Provider shall dispose of or provide a mechanism for the Board to transfer Student Data obtained under the Service Agreement in a usable format, 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 JCPS may employ a **“Directive for Disposition of Data”** form, a copy of which is attached hereto as **Exhibit “D”**. If the JCPS 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”**.
8. **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 Service to the Board. 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 JCPS 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.
9. **Liability.** [intentionally omitted]

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the Board, Provider will provide a list of the locations where Student Data is stored.
2. **Audits.** No more than once each year of the term of this DPA and upon written request from the Board, Provider will provide its security due diligence artifacts, including an updated security posture overview and HECVAT. Provider will cooperate reasonably with the Board 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 the Board 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 standards set forth in **Exhibit “E”**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “E”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who the Board may contact if there are any data security concerns or questions. Additionally, The Provider agrees to maintain a minimum security standard including but limited to the following precautions and protections:
 - a) Encrypting all data, at rest and in transit;
 - b) Maintaining multi-factor authentication on accounts that can access the network or email remotely, including 3rd party accounts;
 - c) Securing access to any physical areas/electronic devices where sensitive data are stored;

- d) Establishing and enforcing well-defined data privilege rights which follow the rule of least privilege and restrict users' access to the data necessary for this to perform their job functions;
- e) Ensuring all staff and 3rd parties sign a nondisclosure statement, and maintaining copies of the signed statements;
- f) Installing end-point protection including but not limited to anti-malware and anti-spyware on any device connected to the network that has access to scoped data, when applicable

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 the Board 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 confirmation 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 individual reporting a breach 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 the Board, upon request, with a summary of said written incident response plan.

- (4) The Board shall provide notice and facts surrounding the breach to the affected students, parents or guardians, or staff, as applicable.
- (5) In the event of a breach originating from the Board's use of the Service, Provider shall cooperate with the Board to the extent necessary to expeditiously secure Student Data.

5. Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act.

If Provider receives Personal Information as defined by and in accordance with the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq. (the "Act"), Provider shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following as applicable:

- a. "Personal Information" is defined in accordance with KRS 61.931(6) as an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
 - i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
 - ii. A Social Security number;
 - iii. A taxpayer identification number that incorporates a Social Security number;
 - iv. A driver's license number, state identification card number or other individual identification number issued by an agency;
 - v. A passport number or other identification number issued by the United States government; or
 - vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.
- b. As provided in KRS 61.931(5), a "non-affiliated third party" means any person or entity that has a contract or agreement with an agency and receives (accesses, collects or maintains) personal information from the agency pursuant to the contract or agreement.
- c. Provider shall not re-disclose, without the written consent of JCPS, any "personal information," as defined in KRS 61.931, or any other personally identifiable information of a student or other persons, such as employees, except as permitted by the Service Agreement.
- d. Provider agrees to reasonably cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act where required.
- e. Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

6. Cloud Computing Service Providers. If Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Provider agrees that, if applicable:

Except as otherwise permitted in the Service Agreement, Provider shall not process Student Data for any purpose other than providing, improving, developing, or maintaining the integrity of its Services that are cloud computing services, unless the provider receives express permission from the student's parent. Provider shall work with the student's school and district to determine the best method of collecting parental permission.pursuant to KRS 365.734(2), Provider shall not in any case process Student Data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.

Pursuant to KRS 365.734(2), Provider shall not sell, disclose, or otherwise process student data for any commercial purpose, except as permitted by the Service Agreement or this DPA.

Pursuant to KRS 365.734(3), Provider shall certify in writing to the agency that it will comply with KRS 365.734(2) as provided in this Section 6.

ARTICLE VI: 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 been terminated. One 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 JCPS'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. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.
4. **Modification.** No waiver, alteration or modification of the provisions of this Agreement shall be binding unless in writing and mutually agreed upon. Any modifications or additions to this Agreement must be negotiated and approved by both parties.
5. **Disputes.** Any differences or disagreements arising between the Parties concerning the rights or liabilities under this DPA, or any modifying instrument entered into pursuant to this DPA, shall be resolved through the procedures set out in the Regulations.
6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or certified mail, sent to the designated representatives below.
- 7.

The designated representative for the Board for this DPA is:

Name: Eric Satterly

Title: Chief Information Officer

Address: 3332 Newburg Road, Louisville, KY 40218

Phone: 502-485-3485

Email:eric.satterly@jefferson.kyschools.us

The designated representative for the Provider for this DPA is:

Name:Spencer Barr Title: Competitive Sales Manager

Address:

600 P Street, Suite #400, Lincoln, NE 68508

Phone: N/A

Email: legal@hudl.com

- 8. **Amendment and Waiver.** 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.
- 9. **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.
- 10. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE COMMONWEALTH OF KENTUCKY, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. ANY PROVISION IN THE SERVICE AGREEMENT REQUIRING VENUE IN A SPECIFIC STATE SHALL NOT APPLY.

11. **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
12. **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.
13. **Relationship of Parties.** The Board is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor the Board shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.
14. **Equal Opportunity.** During the performance of this DPA, Provider agrees that Provider shall not discriminate against any employee, applicant or subcontractor because of race, color, national origin, age, religion, marital or parental status, political affiliations or beliefs, sex, sexual orientation, gender identity, gender expression, veteran status, genetic information, disability, or limitations related to pregnancy, childbirth, or related medical conditions. If the Compensation is paid from federal funds, this DPA is subject to Executive Order 11246 of September 24, 1965 and in such event the Equal Opportunity Clause set forth in 41 Code of Federal Regulations 60-1.4 is hereby incorporated by reference into this DPA as if set forth in full herein.
15. **Prohibition on Conflicts of Interest.** It shall be a breach of this DPA for Provider to commit any act which is a violation of Article XI of the Regulations entitled "Ethics and Standards of Conduct," or to assist or participate in or knowingly benefit from any act by any employee of the Board which is a violation of such provisions.
16. Contractor shall be in continuous compliance with the provisions of KRS Chapters 136, 139, 141, 337, 338, 341, and 342 that apply to Provider for the duration of this DPA and shall reveal any final determination of a violation by the Provider of the preceding KRS chapters.
17. **Access to School Grounds.** No employee or agent of Provider shall access the Board's school grounds on a regularly scheduled or continuing basis for purposes of providing services to students under this DPA.

IN WITNESS WHEREOF, The Board and Provider execute this DPA as of the Effective Date above.

BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY

By: _____ Date: _____
Printed Name: Dr. Brian H. Yearwood _____
Title/Position: Superintendent _____


[Insert Name of Provider] Hudl
By:  _____ Date: 31 March 2026
Printed Name: Spencer Barr _____
Title/Position: Sales Manager _____

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System (Windows)	Check if Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check if Used by Your System (IOS)	Check if Used by Your System (Browser Based)	Check if Used by Your System (Other, please specify: _____)
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc. - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Other application technology meta data- Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Assessment	Standardized test scores (i.e., ACT/SAT) - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries) - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Gender - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System (Windows)	Check if Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check if Used by Your System (iOS)	Check if Used by Your System (Browser Based)	Check if Used by Your System (Other, please specify: _____)
	Other demographic information-Please specify: Age - Optional Photos - Optional Height - Optional Weight - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enrollment	Student school enrollment - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Year of graduation - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Email - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Phone - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Special Indicator	English language Learner information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Medical alerts/ health data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Category of Data	Elements	Check If Used by Your System (Windows)	Check If Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check If Used by Your System (iOS)	Check If Used by Your System (Browser Based)	Check If Used by Your System (Other, please specify: _____)
	Specialized education services (IEP or 504)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Staff Data	First and Last Name - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Email Address - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Staff ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Other information – Please specify	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Student Contact Information	Address - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Email - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Phone - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student Hudl app username - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student Hudl app password - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student Name	First and/or Last - Required	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program- student types 60 wpm, reading program- student reads below grade level)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Student work	Student generated content; comments, pictures, highlights, etc. - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System (Windows)	Check if Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check if Used by Your System (IOS)	Check if Used by Your System (Browser Based)	Check if Used by Your System (Other, please specify: Focus Cameras)
	Other student work data -Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transcript	Student course grades - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student course data - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student course grades/ performance scores - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Other transportation data – Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application:					
	Sports Performance Scores (i.e., 40 Yard Dash, Vertical Leap, Squat, etc.) - Optional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Sports/Academic Awards - Optional					
	Video Footage captured from Focus Cameras - Required					
None	No Confidential Data collected at this time. Provider will immediately notify JCPS if this designation is no longer applicable.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

EXHIBIT "A"**DESCRIPTION OF SERVICES**

Provider shall provide software licenses and support for the following products at prices equal or below Provider's standard pricing rates for the products:

"Services" means the Hudl products and services, including software and hardware for use by its high school sports teams, coaches, athletic department staff, enrolled student athletes, and others as described further in the Service Agreement (defined below).

The Services may include:

- **Capture Solutions** (e.g., Focus cameras for recording games, practice, or other events)
- **Video and Data Analysis Tools** (to break down video from games or practice, apply data, stats, and analytics).
- **Performance Tracking Tools** (for athlete monitoring and data analysis).
- **Recruiting Facilitation Tools** (to assist with athlete promotion and collegiate recruitment).
- **Public Game Livestreaming Tools** (to broadcast games via the Board's school/team account).
- **Public Game Event Ticketing Tools** (e.g., Hudl Tickets, for the Board's administration of event access).
- **Operations Tools** (for team communication, scheduling, and management related to the athletic program).
- Any future products or services that Provider may offer, as added pursuant to Article I, Section 1.2 of the DPA.

For purposes of this DPA, the definition of "Services" **shall not** include:

1. Hudl products and services used by fans of sports teams and fans, viewers, and attendees of athletic and other events.
 - a. For clarity: The tools provided to the **TEAM** to sell tickets or broadcast their events are Services, while an individual's purchase of tickets or livestreams are NOT Services.
2. Any athlete's use of Hudl outside of the Board's subscription (e.g., using Hudl for another team, using Hudl for personal purposes as a fan)

COMPENSATION

Purchase orders shall be entered by each participating school. Funds for purchase shall come from individual school budgets. Total payments under this DPA shall not exceed \$ 8,000.00 per school per fiscal year, running from July 1-June 30.

EXHIBIT “C”
DEFINITIONS

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.

Compensation: Amounts to be paid to the Provider in exchange for software licenses and support. The maximum amount of Compensation that may be paid under this DPA is set forth in Attachment A. The Board is not obligated to pay the maximum Compensation amount solely by its inclusion in this DPA. Compensation owed is determined by the purchase orders submitted to Provider. The cost for any single license or support provided under this DPA shall not exceed Provider’s standard pricing for that product.

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.

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 Board for K–12 school purposes.

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”.

Regulations: The Board Procurement Regulations, available on the JCPS website, as may be amended from time to time.

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 tOrder(s) executed between the Board and Provider and Provider's Organization Terms of Service located 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.

Student Data: Student Data includes any data, whether gathered by Provider or provided by the Board 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.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than Board 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.

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 educational software or services, including cloud-based services, for the digital storage, management, and retrieval of information.

For the purposes of clarity, the definitions of "Educational Records," "Personally Identifiable Information (PII)," and "Student Data" 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 Provider with respect to an individual's direct relationship with Provider including where the individual is interacting with Provider's fan experience.

EXHIBIT “D”

DIRECTIVE FOR DISPOSITION OF DATA

The Board of Education of Jefferson County Kentucky directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between The Board 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]**

Signature

Authorized Representative of the Board

Date

Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT “E”

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

Provider will utilize one of the following known and credible cybersecurity frameworks which can protect digital learning ecosystems.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
	American Institute of CPAs	SOC2
	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
X	The Board of Education of Jefferson County	Board provided standardized questionnaire



Hudl Student Data Protection Agreement

This Hudl Student Data Protection Agreement (this "DPA") is entered into by and between _____, with an address at _____ (the "Organization") and Agile Sports Technologies, Inc. dba Hudl, a Delaware corporation, with an address at 600 P Street, Suite 400, Lincoln, NE 68508 ("Hudl", and together with the Organization, the "Parties" and each a "Party"), effective as of the latest date beneath the signatures in the first Order Form signed by the parties (the "Effective Date").

WHEREAS, Hudl will provide Services to Organization pursuant to the Service Agreement entered into between the Parties;

WHEREAS, the Parties recognize the need to protect Student Data exchanged between them as a result of the Services, 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); and applicable state student privacy laws and regulations; and

WHEREAS, Hudl and Organization wish to enter into this DPA to establish their respective obligations and duties regarding Student Data.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Definitions and Interpretation.

1.1. In addition to other terms defined in this DPA, the following definitions apply in this DPA:

1.1.1. "**Affiliate**" means, in the case of a Party, any other person or entity (a) controlling, (b) controlled by, or (c) under common control with such Party.

1.1.2. "**Agreement**" means this DPA and the Service Agreement.

1.1.3. "**Breach**" means the unauthorized release, disclosure, or acquisition of Student Data that compromises the security, confidentiality, or integrity of the Student Data maintained by Hudl.

1.1.4. "**De-Identified Data**" means all Personally Identifiable Information has been removed or obscured from records and information, 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.

1.1.5. "**Educational Records**" are records, files, documents, and other materials directly related to a student and maintained by the Organization, or by a person acting for such Organization, 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.

1.1.6. "**Metadata**" refers to contextual information associated with collected data, including, but not limited to: timestamps, authorship, and purpose of data generation. Metadata that has been stripped of all direct and indirect identifiers is not considered Personally Identifiable Information.

1.1.7. "**Personally Identifiable Information**" has the definition given to it in 34 C.F.R. § 99.3 and any applicable state law, except as otherwise provided in this DPA.

1.1.8. "**School Official**" means, for the purposes of this DPA, a contractor that: (1) performs an institutional service or function for which the Organization would otherwise use employees; (2) is under the direct control of the Organization with respect to the use and maintenance of Student Data, including Educational Records; and (3) is subject to 34 C.F.R. § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Educational Records.

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



the Services.

- 1.1.10. **"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.
- 1.1.11. **"Student Data"** includes any data, whether gathered by Hudl or provided by Organization 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 Metadata. Student Data further includes Personally Identifiable Information. 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 shall not include that information that has been anonymized or is De-Identified Data or anonymous usage data regarding a student's use of Hudl's services.
- 1.1.12. **"Student-Generated Content"** means materials or content created by a student in the Services and may include, but is not limited to, posts, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.
- 1.1.13. **"Subprocessor"** means a party other than Organization or Hudl that Hudl uses for data collection, analytics, storage, or other service to operate or improve its Services and that has access to Student Data with respect to such services being provided to Hudl.
- 1.1.14. **"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 website, 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 website 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.
- 1.2. The definitions of **"Educational Records"**, **"Personally Identifiable Information"**, and **"Student Data"** 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.
- 1.3. In the case of conflict or ambiguity between:
 - 1.3.1.any provision contained in the body of this DPA and any provision contained in the Exhibits, the provision in the Exhibits of this DPA will prevail; and
 - 1.3.2.any of the provisions of this DPA and the provisions of the Service Agreement, the provisions of this DPA will prevail.
- 1.4. This DPA is subject to the terms of the Service Agreement, made part of, and is incorporated into the Service Agreement by this reference. Interpretations and defined terms set forth in the Service Agreement apply to the interpretation of this DPA, except as otherwise provided herein.
- 1.5. Exhibit "A" attached hereto contains supplemental terms from applicable state law, if any. Exhibit "A" forms part of this DPA and will have the same effect as if set out in full in the body of this DPA. Any reference to this DPA



includes Exhibit "A".

2. **Term and Termination.** This DPA shall remain in effect for three (3) years from the Effective Date. In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent. One party may terminate this DPA upon a material breach of this DPA by the other party by providing written notice to the breaching party. If the Service Agreement terminates, Hudl shall destroy all of Organization's Student Data pursuant to Section 5.6 below.
 3. **Access to Student Data.**
 - 3.1. **FERPA.** For the purposes of FERPA, Hudl will act as a School Official, under the control and direction of the Organization as it pertains to the use of Student Data.
 - 3.2. **Hudl's Access.** Hudl will receive access to Student Data to provide the Services, as described in the Service Agreement. Hudl agrees that all copies of Student Data accessed for the Services, including any modifications or additions to the Student Data, are subject to the provisions of this DPA, and such modifications or additions will be treated in the same manner as the original Student Data. The Student Data shared pursuant to the Service Agreement shall be used for no purpose other than the Services, as stated in the Service Agreement, or as otherwise authorized under the laws and regulations referred to herein this DPA.
 - 3.3. **Subprocessor Access.** Subprocessors may access Student Data for the Services when performing services for Hudl with respect to the Services, provided that Hudl shall enter into written agreements with all such Subprocessors pursuant to which such Subprocessors agree to protect Student Data in a manner no less stringent than the requirements of this DPA.
 - 3.4. **Parent and Student Access.**
 - 3.4.1. To the extent required by applicable law, Organization shall allow a parent, legal guardian, or Eligible Student (as defined under FERPA) to do any of the following, with respect to the Educational Records or Student Data of their student:
 - 3.4.1.1. Review Personally Identifiable Information collected about their student;
 - 3.4.1.2. Correct erroneous information within the collected Personally Identifiable Information of their student; and
 - 3.4.1.3. Transfer Student-Generated Content to a personal account.
 - 3.4.2. The rights set forth in Section 3.4.1. above shall be consistent with the functionality of the Services. When Organization is not able to fulfill such parent, legal guardian, or Eligible Student requests described in Section 3.4.1 on its own through the Services, Hudl agrees to assist with such requests. For such assistance, Organization shall make a written request to Hudl, describing the requested action. Hudl shall use reasonable efforts to respond within 45 days to any such reasonable request by Organization. If a parent or other individual contacts Hudl to review any of the Student Data accessed pursuant to the Services, Hudl shall refer the parent or individual to the Organization, which will direct such individual to follow the necessary and proper procedures regarding the Student Data.
 - 3.5. **Compelled Disclosures.** In the event law enforcement or another government entity requests that Hudl provide such party with Student Data held by Hudl pursuant to the Services, Hudl agrees to notify Organization prior to such compelled disclosure; provided that Hudl shall not be required to provide such notification to Organization in the event Hudl is lawfully directed by such party not to inform Organization of the request or unless Hudl is otherwise legally prohibited from doing so.
 - 3.6. **Data Ownership.** Student Data shared with Hudl pursuant to the Service Agreement is and shall continue to be the property of Organization and Organization shall have control over such Student Data. As between the Parties, all rights in and to such Student Data, including all intellectual property rights therein, shall belong to Organization, subject to the terms of the Service Agreement.
4. **Organization's Responsibilities.** Organization shall comply with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time, when providing Student Data to Hudl for the Services. If the Organization has a policy of disclosing Educational Records or Student Data under FERPA, Organization 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. Organization shall take reasonable



precautions to secure usernames, passwords, and any other means of gaining access to the Services and hosted Student Data. Organization shall notify Hudl promptly of any known unauthorized access. Organization will assist Hudl in any efforts by Hudl to investigate and respond to any unauthorized access.

5. Hudl's Responsibilities.

- 5.1. **Privacy Compliance.** Hudl shall comply with all applicable federal, state, and local laws, rules, and regulations, all as may be amended from time to time, pertaining to Student Data privacy and security.
- 5.2. **Employee Obligations.** Hudl shall require its employees and agents with access to Student Data to comply with the applicable provisions of this DPA. Hudl agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
- 5.3. **No Disclosure.** Hudl will not disclose or share any Student Data except:
 - 5.3.1. As directed or permitted by Organization, this DPA, or the Service Agreement;
 - 5.3.2. As required or permitted by applicable law;
 - 5.3.3. Pursuant to a court order, lawfully issued subpoenas, or other legal process;
 - 5.3.4. When the disclosure consists solely of De-Identified Data;
 - 5.3.5. As necessary to provide the Services; or
 - 5.3.6. To Subprocessors in order for such Subprocessors to perform services on behalf of Hudl with respect to the Services. 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 described in the Service Agreement, or disclosure or provision of an athlete's profile data to verified recruiters, provided such disclosure or provision of profile data is consistent with the athlete's privacy settings.
- 5.4. **Transferring Student-Generated Content.** If Hudl stores or maintains Student-Generated Content, upon request of the Organization, Hudl shall facilitate the transfer of such content to a separate account created by the student, or provide a mechanism for the Organization to transfer said Student-Generated Content.
- 5.5. **De-Identified Data.** Hudl will not attempt to re-identify De-Identified Data or use De-Identified Data for any purpose other than as described in Section 6.5. Hudl will not transfer De-Identified Data to any third parties, except for its Subprocessors and Affiliates, unless (1)(a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the Organization, who has provided written consent for such transfer, or (2) such De-Identified Data has been sufficiently aggregated that it cannot be re-identified.
- 5.6. **Disposition of Data.** Upon written request from Organization, Hudl shall delete or provide a mechanism for Organization 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 delete Student Data shall not extend to De-Identified Data or Student Data placed in a separate student account pursuant as allowed herein.
- 5.7. **Advertising Limitations.** Hudl will not use, disclose, or sell Student Data for any Targeted Advertising or to develop a profile of a student or family member/guardian for any commercial purpose other than providing the Services or as permitted by the Service Agreement. This section does not prohibit Hudl from using Student Data (1) for adaptive learning or customized student learning (including generating personalized learning recommendations); (2) to make product recommendations to teachers or Organization employees; or (3) 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, if any.

6. Data.

- 6.1. **Data Storage.** Hudl will provide a list of the locations where Student Data is stored upon written request of the Organization. Hudl will store all Student Data in the United States where required by applicable law.
- 6.2. **Audits.** No more than once each year of the term of this DPA, and upon written request from the Organization, Hudl will provide its security due diligence artifacts, including an updated security posture overview and HECVAT. Hudl will cooperate reasonably with the Organization and any local, state, or federal agency with



oversight authority or jurisdiction in connection with any audit or investigation of Hudl or delivery of Services to students or Organization as required by applicable law.

6.3. **Data Security.** Hudl shall adhere to any applicable law relating to data security. Hudl agrees to use reasonable and appropriate administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. Upon reasonable written request, Hudl shall provide contact information of a Hudl employee who Organization may contact if there are any data security concerns or questions.

6.4. **Data Breach.**

6.4.1. In the event of a Breach, Hudl shall provide notification to Organization within seven (7) days of confirmation of the Breach, unless notification within this time limit would disrupt investigation of the Breach by law enforcement. The Breach notification shall include, at a minimum, the following information, to the extent known by Hudl and as it becomes available:

6.4.1.1. A list of the types of Student Data that were or are reasonably believed to have been the subject of a Breach;

6.4.1.2. The date, estimated date, or date range within which the Breach occurred;

6.4.1.3. Whether the notification was delayed because of a law enforcement investigation; and

6.4.1.4. A general description of the Breach, if that information is possible to determine at the time the notice is provided.

6.4.2. Hudl agrees to adhere to all applicable federal and state requirements with respect to a Breach, including, any required notification or mitigation.

6.4.3. Hudl agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and applicable federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data, and Hudl agrees to provide Organization with a summary of its written incident response plan upon written request.

6.4.4. Organization shall provide notice of the Breach to affected students, parents, or guardians.

6.5. **Using De-Identified Data.** De-Identified Data may be used by Hudl and its Subprocessors for the following: (1) any purposes allowed under FERPA; (2) improvement, research, and development of Hudl's sites, services, and applications, and to demonstrate the effectiveness of the Services; and (3) adaptive learning and customized student learning. Hudl's use of De-Identified Data shall survive termination of this DPA, and Hudl shall not be required to return or destroy De-Identified Data.

7. **Miscellaneous.**

7.1. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersede 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.

7.2. **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.

7.3. **Severability.** If any term or provision of this DPA is invalid, illegal, or unenforceable in any jurisdiction, such invalidity, illegality, or unenforceability shall not affect any other term or provision of this DPA or invalidate or render unenforceable such term or provision in any other jurisdiction. Upon such determination that any term or other provision is invalid, illegal, or unenforceable, the parties hereto shall negotiate in good faith to modify this DPA to reflect the original intent of the parties as closely as possible in a mutually acceptable manner in order



that the transactions contemplated hereby be consummated as originally contemplated to the greatest extent possible.

- 7.4. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE NEBRASKA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES OF SUCH STATE. IF ORGANIZATION IS A STATE OR LOCAL GOVERNMENT ENTITY (SUCH AS A PUBLIC SCHOOL OR PUBLIC SCHOOL DISTRICT), THE PROVISION IN THIS DPA ADDRESSING GOVERNING LAW WILL NOT APPLY TO ORGANIZATION TO THE EXTENT ORGANIZATION'S JURISDICTION'S LAWS PROHIBIT ORGANIZATION FROM ACCEPTING THAT PROVISION. ANY PROVISION IN THE SERVICE AGREEMENT REQUIRING VENUE IN A SPECIFIC STATE SHALL NOT APPLY.
- 7.5. **Successors Bound.** This DPA is and shall be binding upon the respective successors in interest to Hudl 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.
- 7.6. **Authority.** Each party represents that it has the right, power, and authority to enter into this DPA, become a Party hereto, and perform its obligations hereunder, including confidentiality and destruction of Student Data.
- 7.7. **Notices.** Each party shall deliver all notices, requests, consents, claims, demands, waivers, and other communications under this DPA (each, a "Notice") in writing. Each party shall deliver all Notices by personal delivery, nationally recognized overnight courier (with all fees prepaid), email (with confirmation of transmission), or certified or registered mail (in each case, return receipt requested, postage prepaid). All communications to Organization, including those related to Organization's account, shall be sent to the applicable Team Admin on file. Organization shall send notices or communications intended for Hudl to the address set forth for Hudl above. Organization shall also provide a copy to the attention of Hudl Legal at legal@hudl.com. Except as otherwise provided in this Agreement, a Notice is effective only upon receipt by the receiving party. Either party may change its address for notices under this Agreement by giving written notice to the other party by the means specified in this Section.
- 7.8. **Counterparts.** This DPA may be executed in counterparts, each of which shall be deemed an original, but all of which together shall be deemed to be one and the same agreement. A signed copy of this DPA delivered by email or other means of electronic transmission shall be deemed to have the same legal effect as delivery of an original signed copy of this Agreement.

IN WITNESS WHEREOF, Organization and Hudl have executed this DPA as of the Effective Date.

_____, Organization

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

Agile Sports Technologies, Inc., dba Hudl

By: _____ Date: _____

Printed Name: _____ Title/Position: _____



EXHIBIT "A"

Supplemental State Terms for _____