

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT
Version 1.0

Atascadero Unified School District

and

DragonFly Athletics, LLC

7/30/2018

This California Student Data Privacy Agreement ("DPA") is entered into by and between the Atascadero Unified School District (hereinafter referred to as "LEA") and DragonFly Athletics, LLC (hereinafter referred to as "Provider") on 05/07/2018. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Education Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated 07/01/2018 ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive and the LEA may provide documents or data that are covered by several federal and statutes, among them, the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. 1232g, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h; and

WHEREAS, the documents and data transferred from California LEAs are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (sometimes referred to as either "SB 1177" or "SOPIPA") found at California Business and Professions Code section 22584; and

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

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

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

ARTICLE I: PURPOSE AND SCOPE

- 1. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable privacy statutes, including the FERPA, PPRA, COPPA, SB 1177 (SOPIPA), and AB 1584. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.
- 2. Nature of Services Provided.** The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

3. **Student Data to Be Provided.** In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as **Exhibit "B"**:

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

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data or any other Pupil Records 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 Parties agree that as between them all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.
2. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records of Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
3. **Separate Account.** Provider shall, at the request of the LEA, transfer Student generated content to a separate student account.
4. **Third Party Request.** Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.

5. **No Unauthorized Use.** Provider shall not use Student Data or information in a Pupil Record for any purpose other than as explicitly specified in the Service Agreement.
6. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree protect Student Data in manner consistent with the terms of this DPA

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA.** LEA shall provide data for the purposes of the Service Agreement in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232 g, AB 1584 and the other privacy statutes quoted in this DPA.
2. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
3. **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.
4. **District Representative.** At request of Provider, LEA shall designate an employee or agent of the District as the District representative for the coordination and fulfillment of the duties of this DPA.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all California and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRRA, AB 1584, and SOPIPA.
2. **Authorized Use.** The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above.
3. **Employee Obligation.** Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of FERPA laws with respect to the 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.** Provider shall not disclose any data obtained under the Service Agreement in a manner that could identify an individual student to any other entity in published results of studies as authorized by the Service Agreement. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services, or applications.

5. **Disposition of Data.** Provider shall dispose of all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within 60 days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

6. **Advertising Prohibition.** Provider is prohibited from using Student Data to conduct or assist targeted advertising directed at students or their families/guardians. This prohibition includes the development of a profile of a student, or their families/guardians or group, for any commercial purpose other than providing the service to client. This shall not prohibit Providers from using data to make product or service recommendations to LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Provider agrees to abide by and maintain adequate data security measures to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in in Exhibit "D" hereto. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Provider shall make best efforts practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.
 - b. **Destruction of Data.** Provider shall destroy all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was

obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

- c. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.
- d. **Employee Training.** The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.
- e. **Security Technology.** When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology protects information, using both server authentication and data encryption to help ensure that data are safe secure only to authorized users. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
- f. **Security Coordinator.** Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement
- g. **Subprocessors Bound.** Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

- 2. **Data Breach.** In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident. Provider shall follow the following process:
 - a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.
 - b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information 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.
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- c. At LEA's discretion, the security breach notification may also include any of the following:
- i. Information about what the agency has done to protect individuals whose information has been breached.
 - ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.
- d. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts.
- e. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: GENERAL OFFER OF PRIVACY TERMS

Provider may, by signing the attached Form of General Offer of Privacy Terms ("General Offer"), (attached hereto as Exhibit "E"), be bound by the terms of this DPA 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. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.
2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.
3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall

destroy all of LEA's data pursuant to Article V, section 1(b).

4. **Priority of Agreements.** This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and the Service Agreement, 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.
5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the addresses set forth herein.
6. **Application of Agreement to Other Agencies.** Provider may agree by signing the General Offer of Privacy Terms be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.
7. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
8. **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.
9. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA,

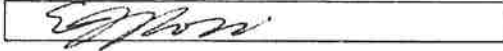
WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS LOCATED IN San Luis Obispo COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

[Signature Page Follows]

Attached Addendum to California State Data Privacy Agreement is incorporated by reference and is a part of the agreement between the parties as if fully set forth in this document. XJCS

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

Atascadero Unified School District

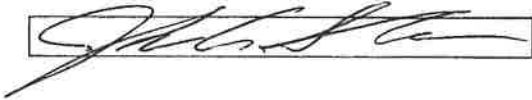


Date: 6.1.18

Printed Name: EJ Rossi

Title/Position: Assistant Superintendent of Instructional Services

DragonFly Athletics, LLC



Date: 7/30/2018

Printed Name: Clint Sanders

Title/Position: Product Manager

Note: Electronic signature not permitted.

EXHIBIT "A"
DESCRIPTION OF SERVICES

DragonFly MAX is an athlete-centered electronic health record focused on improving health, performance, & communication. DragonFly MAX helps you get in the game & stay in the game by:

- * Simplifying the School Forms Process for Parents & Schools
- * Making Injury Documentation Easy for Healthcare Providers
- * Communicating Seamlessly to Everyone Involved in Athlete Care

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	<input checked="" type="checkbox"/>
	Other application technology meta data-Please specify	<input checked="" type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input checked="" type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications that are captured (emails, blog entries)	<input checked="" type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
Demographics	Date of Birth	<input checked="" type="checkbox"/>
	Place of Birth	<input checked="" type="checkbox"/>
	Gender	<input checked="" type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, preferred or primary language spoken by student)	<input type="checkbox"/>
	Other demographic information-Please specify	<input checked="" type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input checked="" type="checkbox"/>
Other enrollment information-Please specify	<input type="checkbox"/>	
Parent/Guardian Contact Information	Address	<input checked="" type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input checked="" type="checkbox"/>

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts	<input checked="" type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify	<input type="checkbox"/>
Category of Data	Elements	Check if used by your system
Student Contact Information	Address	<input checked="" type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input checked="" type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input checked="" type="checkbox"/>
	Vendor/App assigned student ID number	<input checked="" type="checkbox"/>
	Student app username	<input checked="" type="checkbox"/>
	Student app passwords	<input checked="" type="checkbox"/>
	Student Name	First and/or Last
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input checked="" type="checkbox"/>
Student work	Student generated content writing, pictures etc	<input type="checkbox"/>

Category of Data	Elements	Check if used by your system
Other	Other student work data - Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/performance scores	<input type="checkbox"/>
	Other transcript data -Please specify	<input type="checkbox"/>

Category of Data	Elements	Check if used by your system
Transportation	Student bus assignment	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>
	Other transportation data - Please specify	<input type="checkbox"/>
Other	Please list each additional data element used, stored or collected by your application	<input type="checkbox"/>

EXHIBIT "C"

DEFINITIONS

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

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

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: For the purposes of SB 1177, SOPIPA, the term "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 primarily for K–12 school purposes and was designed and marketed for K–12 school purposes. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in AB 1584.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First and Last Name	Home Address
Telephone Number	Email Address
Discipline Records	Test Results
Special Education Data	Juvenile Dependency Records
Grades	Evaluations
Criminal Records	Medical Records
Health Records	Social Security Number
Biometric Information	Disabilities
Socioeconomic Information	Food Purchases
Political Affiliations	Religious Information
Text Messages	Documents
Student Identifiers	Search Activity
Photos	Voice Recordings
Videos	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the Service Agreement the term "Provider" replaces the term "Third Party as defined in California Education Code § 49073.1 (AB 1584, Buchanan), and replaces the term as "Operator" as defined in SB 1177, SOPIPA.

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

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational LEA employee.

SB 1177, SOPIPA: Once passed, the requirements of SB 1177, SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

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

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

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and Federal laws and regulations. Student Data as specified in [Exhibit B](#) is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

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

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection,

analytics, storage, or other service to operate and/or improve its software, and who has access to PII. This term shall also include in it meaning the term "Service Provider," as it is found in SOPIPA.

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

Third Party: The term "Third Party" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"
DATA SECURITY REQUIREMENTS

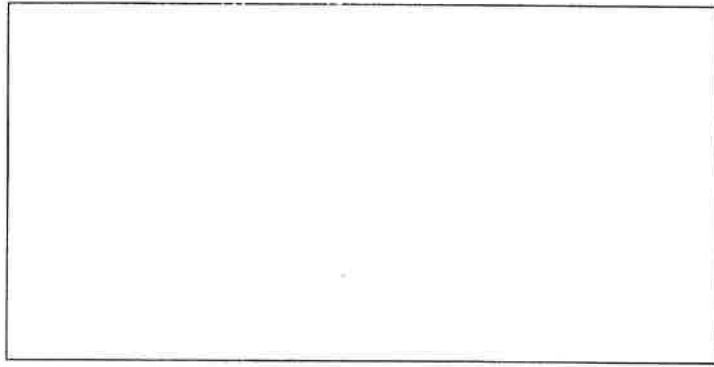


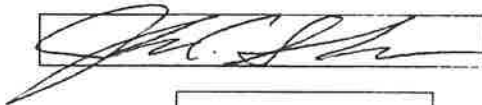
EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Atascadero USD and which is dated 7/30/2018 to any other LEA ("Subscribing LEA") to anyone who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the other LEA may also agree to change the data provided by LEA to the Provider to suit the unique needs of the LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statutes; (2) a material change in the services and products listed in the Originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Provider shall notify the California Student Privacy Alliance in the event of any withdrawal so that this information may be transmitted to the Alliance's users.

DragonFly Athletics, LLC



Printed Name: Clint Sanders

Date: 7/30/2018

Title/Position: Product Manager

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA.

Printed Name:

Date:

Title/Position:

ADDENDUM TO California Student Data Privacy Agreement

This Addendum amends and adds to the CSDPA between DragonFly Athletics, LLC ("DragonFly") and Ascalando Unified School District ("Local Education Agency" or "LEA").

1. Privacy and Data Security. To protect the privacy of its users and the confidentiality of health information and other student-athlete information, DragonFly restricts access to a student's records to only the LEA, the student or student's parent/guardian, and any person that the LEA or student/student's parent or guardian authorizes for access. DragonFly is not responsible for access given to student records by the LEA, the student, the student's parent or guardian, or some other person authorized by one those (for example, a trainer affiliated with the LEA). DragonFly performs its risk management process in accordance with NIST SP 800-30. DragonFly aligns its Information Security Management System and related controls with ISO 27001:2013, ISO27002 and ISO27017:2015. DragonFly has a business associate agreement (BAA) with Amazon Web Services. DragonFly MAX runs on Amazon's BAA authorized service layer. Information entered into the DragonFly system by parents, guardians, or student athletes is categorized as a personal health record (PHR) in connection with Federal Trade Commission guidance associated with mobile health applications. Information entered by LEA administrators are student records and align with the Family Educational Rights and Privacy Act (FERPA). The Health Insurance Portability and Accountability Act (HIPAA) regulatory framework does not apply to student records, but DragonFly protects health information under HIPAA-compliant standards. Student medical treatment records that a student authorizes to be released to entities outside of the school are no longer under the school's authority and become the responsibility of the recipient. DragonFly MAX assists students, parents, LEAs, and those affiliated with LEAs or students (such as leagues, coaches, athletic trainers, schools, and teams) provide required forms and personal health record information to affiliated athletic trainers and allows athletic trainers to update the status of an athlete's injuries. Because student records are covered by FERPA, there is no need to submit a BAA to DragonFly. The LEA is responsible for ensuring compliance with any privacy laws or rules by the coaches, trainers, or other individuals it authorizes to have access to a student athlete's information through the DragonFly services. Nothing in the agreement between DragonFly and the LEA, and nothing in DragonFly's Terms of Use or privacy policies, should be understood or construed as DragonFly voluntarily opting to be subject to any federal, state, or local laws that would not otherwise apply to DragonFly absent the agreement, Terms of Use, or policies.

2. No Medical Services Provided. DragonFly provides no training services, physical therapy, or other healthcare services. DragonFly is not responsible and makes no representations or warranties regarding the ability, training, skills, or competence of any trainer, coach, or other person given access to the DragonFly services by an LEA, student athlete, parent, or guardian. Neither DragonFly nor any of its subsidiaries or affiliates or any third party who may promote the DragonFly services or provide a link to the DragonFly services may be held liable for any professional or healthcare advice obtained from a trainer in conjunction with the DragonFly services. DragonFly does not endorse any specific tests, physical therapists, athletic trainers, medications, products, or procedures recommended by trainers, coaches, or other LEA representatives who may use the DragonFly services. DragonFly does not provide and does not intend to provide any medical advice, diagnosis, or recommendations of any kind related to the DragonFly services or any DragonFly site. Never should any content or information transmitted to or from, or stored in, the DragonFly services or on a DragonFly site be interpreted as medical advice or a recommendation of any kind from DragonFly. The LEA acknowledges that while DragonFly may be providing services, the availability of its platform should not be construed as interpreting DragonFly to be a "school official" as that term has been interpreted under FERPA and implementing regulations. Therefore, posting information on DragonFly's platform to be accessed by trainers, coaches, or other LEA representatives may not be construed as subjecting DragonFly to the conditions and limitation of 34 C.F.R. §§ 99.31, 99.33, or other FERPA provisions or regulations. Individual users may authorize or revoke sharing of information with LEAs and others during enrollment,

after enrollment, or when enrolling with a new LEA or other entity. DragonFly may promote or advertise other services or products of DragonFly or affiliates of DragonFly or third parties, but no student athlete's information will be shared by DragonFly with any other entity for marketing. DragonFly accepts an LEA's verification that an athletic trainer is affiliated with the LEA, and DragonFly is not responsible for errors or misinformation provided to DragonFly by an LEA that results in unauthorized disclosure of personal health record information.

3. DragonFly's Terms of Use Remain Applicable. Nothing in this Addendum or in the agreement to which this Addendum relates may be construed as altering or eliminating any of the provisions of the Terms of Use found on the dragonflymax.com website. Those Terms of Use are incorporated by reference in this Addendum and are part of the agreement between DragonFly and the LEA. The Terms of Use apply and govern the obligations and responsibilities of DragonFly and obligations and responsibilities of the users (including the LEA, agents or affiliates of the LEA, students, parents/guardians, or any authorized third parties) of the DragonFly products, services, applications, and websites owned or controlled by DragonFly, including security, data storage and access, compliance with applicable laws, and use of DragonFly mobile applications and websites. Nothing in the agreement between the LEA and DragonFly imposes any binding obligations on DragonFly that are not contained in those Terms of Use and that would not otherwise be imposed by law. The Terms of Use apply to all users, regardless of whether the user is (i) a student athlete, or parent/guardian of a student athlete, (ii) an athletic trainer, sports trainer, physical therapist, or other individual involved with the training or care of a student athlete, or (iii) a representative of a student athlete's or a trainer's school, LEA, or other group, such as a coach, assistant coach, volunteer coach or administrator. To the extent those Terms of Use contradict anything in this Addendum or the agreement to which this Addendum relates, the Terms of Use will govern. The Terms of Use may be amended by DragonFly.

4. Liability and Dispute Resolution. To the fullest extent permitted by law, in no event may DragonFly (or its affiliates, employees, members, owners, or representatives) be responsible or liable to any person or entity for any direct, indirect, incidental, consequential, special, exemplary, punitive, or other losses, liabilities, costs, claims, expenses or damages whatsoever (including, without limitation, those resulting from lost profits, lost data, or business interruption) arising out of or relating in any way to the DragonFly services or the DragonFly sites, whether based on warranty, contract, tort (including negligence), or any other legal theory and whether or not advised of the possibility of such damages. The LEA agrees to defend, indemnify, and hold harmless DragonFly, its affiliates, and the managers, members, officers, representatives, partners, licensors and agents of DragonFly and its affiliates (the DF Parties) from and against all third-party claims, damages, and expenses (including reasonable attorneys' fees) against or incurred by any of the DF Parties due to, related to, or arising out of the LEA's breach of the agreement between LEA and DragonFly (including this Addendum and any documents incorporated by it) or violation of applicable law, any LEA or LEA representative's use or access of the DragonFly services, or the use or access by anyone accessing the DragonFly services using LEA-provided access. In the event of any dispute or claim relating to the DragonFly services or any DragonFly site or the agreement between the LEA and DragonFly (including this Addendum and any documents incorporated by it), the LEA agrees to resolution of such dispute solely in the state courts located in Tuscaloosa County, Alabama, and that the rights and obligations of the parties will be governed by and in accordance with the laws of the State of Alabama, without regard to its conflict of laws principles. The LEA waives any objection to venue and jurisdiction in such courts. Subject to any applicable limitation of liability set forth herein, the rights and remedies herein of DragonFly are cumulative and in addition to any and all rights and remedies that may be provided by law or equity.

5. Noninterference, Warranties, and Severability. The LEA agrees not to use any device, software, or routine to interfere or attempt to interfere with the proper working of DragonFly services or any activity being conducted on any DragonFly site. The LEA and any

representatives of the LEA are prohibited from violating or attempting to violate the security of the DragonFly services, including, without limitation: (a) accessing data not intended for the LEA or logging onto a server or an account which the LEA is not authorized to access; or (b) attempting to probe, scan, or test the vulnerability of a system or network or to breach security or authentication measures without proper authorization; or (c) accessing or using DragonFly services or any portion thereof without authorization, in violation of the Terms of Use, or in violation of applicable law. DragonFly strives to provide a user-friendly, bug-free interface for its users with no downtime on its systems. DragonFly does not warrant that the DragonFly services or any DragonFly site will meet the LEA's requirements or will be uninterrupted or error-free, or that defects in the DragonFly services or any DragonFly site will be corrected. To the extent permitted by applicable law, the DragonFly services and the DragonFly site or sites are provided without warranty, express or implied, of any kind (including without any warranty of merchantability or fitness for a particular purpose). The LEA and users of the DragonFly services and sites assume total risk in the use of the services and the sites. The LEA, for itself and its representatives (including trainers it authorizes), represents and warrants that all user information collected and obtained through the DragonFly services will be kept confidential and will only be disclosed to other parties outside the DragonFly platform as authorized by law. DragonFly reserves the right to terminate access to all or part of DragonFly services, with or without cause, and with or without notice. In the event that any of the agreement between DragonFly and the LEA (including this Addendum) are held by a court or other tribunal of competent jurisdiction to be unenforceable, such unenforceable provisions will be limited or eliminated to the minimum extent necessary so that the agreement between the LEA and DragonFly otherwise remains in full force and effect so as to effect the intent of the agreement will continue in full force and effect.

By signing below, the representative acknowledges agreement to the terms set forth above and that he or she is authorized to sign on behalf of and bind the entity for which he or she is a representative:

DragonFly Athletics, LLC

By: 

Printed name: John C. Sanders

Title: Product Manager

Date: 7/30/2018

[LEA] _____

By: _____

Printed name: _____

Title: _____

Date: _____