



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and ArbiterSports ("Vendor") are parties to a contract dated 07/01/22 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, Arbiter Registration ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

- 2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.
- 2.2. "Vendor" means ArbiterSports.
- 2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.
- 2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.
- 2.5. "Parent" means a parent, legal guardian, or person in parental relation to a Student.
- 2.6. "Student" means any person attending or seeking to enroll in an educational agency.
- 2.7. "Eligible Student" means a student eighteen years or older.
- 2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.
- 2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to this Addendum.

Family ID / Arbiter Sports



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

- 7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.
- 7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.
- 7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.
- 7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

10. Protected Information and Contract Termination

- 10.1. The expiration date of this Contract is defined by the underlying contract.
- 10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.
- 10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.
- 10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.
- 10.5. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.
- 10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

- 11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).
- 11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

- 12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.
- 12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:
- 12.3. align with the NIST Cybersecurity Framework 1.0;
- 12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;
- 12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);
- 12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;
- 12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;
- 12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;



Educational
Technology Service
Genesee Valley
Wayne Finger Lakes

- 12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;
- 12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and
- 12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated or expires.

13. Additional Vendor Responsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

- 13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;
- 13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;
- 13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;
- 13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;
- 13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);
- 13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the Vendor or its Assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Signatures

For Wayne-Finger Lakes BOCES/EduTech

For (Vendor Name) FamilyID, Inc

[Handwritten signature]

DocuSigned by:
John Hopkins
CA64377CAC1D4C5...

Date

7/6/22

Date

6/29/2022



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech) seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech) seeks to insure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the Wayne-Finger Lakes BOCES (EduTech) has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Board Policy 5500 entitled Family Educational Rights and Privacy Act (FERPA).
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at <http://www.nysed.gov/data-privacy-security/student-data-inventory> and a copy may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech

For (Vendor Name) FamilyID, Inc

[Handwritten Signature]
Date 7/6/22

DocuSigned by:
John Hopkins
CAB4377CAC1D4C5

Date 6/29/2022



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

- b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).
- c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

- a) Written notice;
- b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.

The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627



Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment C – Vendor’s Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attached)

ArbiterSports, LLC

Data Privacy and Security

NY Addendum to Terms of Service and Privacy Policy

<https://www.familyid.com/pages/terms-of-service>

<https://www.familyid.com/pages/privacy-policy>

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information, and in 2020 new Part 121 regulations were added. In order to comply with the requirements of Education Law 2-d and Part 121, ArbiterSports hereby establishes the following data security and privacy plan:

ArbiterSports will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. ArbiterSports shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. ArbiterSports shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement or provided for by agreement with the owner of Protected Data. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, ArbiterSports shall have in place sufficient internal controls to ensure that District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, CIPA, FERPA and HIPAA, if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by District. Protected Data also includes any information protected under Education Law 2-d and Part 121 including, but not limited to:

"Personally identifiable information" from student records of District as that term is defined in §99.3 of the Family Educational Rights and Privacy Act (FERPA),

-AND-

Personally identifiable information from the records of District relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law 3012-c and 3012-d.

ArbiterSports has adopted the NIST Cybersecurity Framework and follows NIST 800-53 standards for all controls within its policies. All officers, employees, and contractors who have access to student data will receive training on the federal and state laws governing confidentiality of such data.

State, federal, and local data security and privacy contract requirements will be implemented by utilizing best practices and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site

records, and limitations of access to stored data to authorized staff shall be implemented as follows:

- Servers used by ArbiterSports are configured in accordance with SSL/TLS best practices. The company's SSL validator gives it an A+ rating.
- Protected Data is stored in multiple databases and access to data is strictly controlled with layers of safeguards.
- Servers used by ArbiterSports leverage Azure Virtual Network functionalities and separate our network traffic from other Azure customers.
- Formal security audits are performed by ArbiterSports partners. Internal reviews of policies and procedures that are not covered in those audits are performed annually.
- ArbiterSports automatically encrypts all sensitive information sent to and from our servers. access is password protected using industry best-practice encryption methods: salting & hashing.
- Maintaining the confidentiality, integrity, availability and regulatory compliance of Non-Public Information stored, processed and/or transmitted at ArbiterSports is a requirement of all Authorized Users. This policy applies to information in any format, including electronic and hard copy.
- To safeguard participants/registrants against identity theft, every registration through ArbiterSports is followed by an email confirming the transaction.
- ArbiterSports requires a minimum of TLS 1.2 or for all services.
- In addition to encryption during transit, data stored in ArbiterSports databases is fully encrypted while at rest.
- ArbiterSports utilizes the world-class security, dependability, and scalability of Microsoft Azure Cloud services.

Measures to secure Protected Data and to limit access to such data to authorized staff will include:

- Measures will include all above-mentioned measures, and in addition all Protected Data is accessible only through a password-protected platform and only authorized users have access. Access rights are revoked upon termination of the relationship.
- Subcontractors, persons or entities with which ArbiterSports will share Protected Data, if any, will abide by the requirements of this data security and privacy plan, and any contractual obligations with respect to Protected Data set forth in the agreement with the disclosing party.
- Internal access to Protected Data shall be limited to those individuals that are determined to have legitimate educational interests.
- Protected Data shall not be used for any other purposes than those explicitly authorized by contract with an educational agency or by agreement with the owner of Protected Data.
- Protected Data shall not be re-disclosed to any third party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the party provides a notice of the disclosure to the New York State Education Department, educational agency, or institution that provided the information no later than

the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;

- Reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of Protected Data shall be maintained.
- Encryption technology shall be used to protect data while in motion or in ArbiterSports custody from unauthorized disclosure.

Upon termination or expiration of this agreement, the District can request Protected Data provided by and owned by the District be transitioned to a successor contractor, or deleted or destroyed. Protected Data ownership is further clarified as follows:

- Families and individuals who use ArbiterSports accept the service's Terms and Conditions as part of the service registration process. These Terms, located at <https://hello.familyid.com/terms-of-service>, describe the registrant's rights and obligations relating to the use of the service and they constitute an agreement between the Provider and the registrant. In connection with their registration and use of the service, registrants (who may include members of participating families, parents of students, coaches and others) provide personal information about themselves and their children or other students. This information includes names, addresses, telephone numbers and the like. The registrants are responsible for all information that they provide to the service, and as listed in the Terms, they retain all ownership rights in that information. Since the ArbiterSports service enables registrants to use the service for different organizations (like other schools, camps, sports teams, etc.) they may decide to continue using the service even though they are no longer involved with the District. The registrants can maintain their information on the service, update the information or delete the information at their discretion.
- Notwithstanding anything to the contrary in this agreement, for purposes of the agreement, Student Data, Pupil Records or other similar terms defined or referenced in the agreement that include information relating to individuals or families who use the ArbiterSports service shall only include information that is provided by the District. These terms shall not apply to information that is provided to the service by registrants or their related users, which will remain the sole and exclusive property of such registrants. The agreement shall not in any way require ArbiterSports to delete any such information or take any particular actions with respect to such information. In the event of any conflict between the agreement and the foregoing terms, these terms shall apply.

Certificate Of Completion

Envelope Id: 167C0EE3CDC14E409A24B0494223742F	Status: Completed
Subject: Please DocuSign This Document	
Source Envelope:	
Document Pages: 14	Signatures: 2
Certificate Pages: 1	Initials: 0
AutoNav: Enabled	Envelope Originator:
Envelope Stamping: Enabled	Doug Clawson
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	1 Falconwood Lane
	Sandy, UT 84092
	doug.clawson@arbitersports.com
	IP Address: 64.207.219.9

Record Tracking

Status: Original	Holder: Doug Clawson	Location: DocuSign
6/28/2022 5:39:29 PM	doug.clawson@arbitersports.com	

Signer Events

John Hopkins
john.hopkins@arbitersports.com
CFO
FamilyID, Inc
Security Level: Email, Account Authentication (None)

Signature

DocuSigned by:

CAB4377CAC1D4C5
Signature Adoption: Pre-selected Style
Signed by link sent to
john.hopkins@arbitersports.com
Using IP Address: 24.11.121.81

Timestamp

Sent: 6/28/2022 5:41:40 PM
Viewed: 6/29/2022 7:24:32 AM
Signed: 6/29/2022 7:24:39 AM

Electronic Record and Signature Disclosure:
Not Offered via DocuSign

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	6/28/2022 5:41:40 PM
Certified Delivered	Security Checked	6/29/2022 7:24:32 AM
Signing Complete	Security Checked	6/29/2022 7:24:39 AM
Completed	Security Checked	6/29/2022 7:24:39 AM
Payment Events	Status	Timestamps

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE:** The exclusive purposes for which “student data” or “teacher or principal data” (as those terms are defined in Education Law Section 2-d and collectively referred to as the “Confidential Data”) will be used by ArbiterSports (the “Contractor”) are limited to the purposes authorized in the contract between the Contractor and the Wayne-Finger Lakes BOCES/EduTech (the “BOCES”) dated 07/01/2022 the “Contract”).
2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., the Family Educational Rights and Privacy Act (“FERPA”); Education Law §2-d; 8 NYCRR Part 121).
3. **CONTRACT PRACTICES:** The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in the specified format and/or destroyed by the Contractor as directed by the BOCES.
4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any “education record”, as that term is defined in FERPA, stored by the BOCES in a Contractor’s product and/or service by following the BOCES’ procedure for requesting the amendment of education records under FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by the BOCES in Contractor’s product and/or service by following the appeal procedure in the BOCES’ APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.
5. **SECURITY PRACTICES:** Confidential Data provided to Contractor by the BOCES will be stored in Azure Cloud Services. The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
6. **ENCRYPTION PRACTICES:** The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.