



Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892

Title: Executive Director

Title: CFO

Address: 355 Harlem Rd

Address: 9815 S Monroe St, #204, Sandy, UT 84070

West Seneca, NY 14224

Date: 5/18/2023

**EXHIBIT D**

**DATA SHARING AND CONFIDENTIALITY AGREEMENT**

INCLUDING  
PARENTS BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY  
AND  
SUPPLEMENTAL INFORMATION ABOUT THE MLSA

**1. Purpose**

- (a) This Exhibit supplements the Master License and Service Agreement (“MLSA”) to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES’ Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES’ website.
- (b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service (“TOS”) that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

**2. Definitions**

Any capitalized term used within this Exhibit that is also found in the MLSA will have the same definition as contained within the MLSA.

In addition, as used in this Exhibit:

- (a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (b) “Teacher or Principal Data” means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections

3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

- (c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.
- (d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with a RICS, and as a result is licensed to use Vendor's Product pursuant to the terms of the MLSA. For purposes of this Exhibit, the term also includes Erie 1 BOCES or another RIC that is licensed to use Vendor's Product pursuant to the MLSA to support its own educational programs or operations.

### 3. **Confidentiality of Protected Data**

- (a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.
- (b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy.. Erie 1 BOCES will provide Vendor with a copy of its policy. Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

### 4. **Data Security and Privacy Plan**

Vendor agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with Erie 1 BOCES' Parents Bill of Rights for Data Privacy and Security, a copy of which has been signed by the Vendor and is set forth below.

Additional elements of Vendor's Data Security and Privacy Plan are as follows:

- (a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.
- (b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative,

technical, operational and physical safeguards and practices in place throughout the term of the MLSA:

- a. In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance.
- b. In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the MLSA, Vendor will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the MLSA:

Vendor will adhere to the principles established in the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 to ensure all confidential data collected through the Vendor applications is protected and secured. All controls within the Vendor privacy policies follow the NIST 800-53 standards. Vendor shall not use "Protected Data" (as defined above) for any other purposes than those explicitly provided for in this Agreement or provided for by agreement with the owner of the Protected Data. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Vendor 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.

Connections to Vendor are always encrypted using TLS/SSL between users and our cloud infrastructure, and all data storage, backups, and read-replicas are encrypted using the industry standard AES-256 encryption algorithm. Data is stored in multiple databases that all reside on private networks within our cloud infrastructure, and data is never distributed, used, or accessed outside the private cloud. Vendor has industry-standard policies and procedures that protect the privacy of our users, and all employees are trained on those policies. Vendor also works with Premier AWS Partners to review best practices and ensure we keep current with industry standards.

- Vendor employees and contractors who have access to non-public information stored by our application must submit to a background check, complete training on security practices, and agree to Vendor's privacy policies. All Authorized Users are trained to maintain the confidentiality, integrity, availability, and regulatory compliance of non-public information in any format, including electronic and hard copy.

- All connections to Vendor infrastructure are always encrypted between endpoints using TLS/SSL, and all sensitive information is encrypted when stored.
- All Protected Data is stored in Vendor's virtual private cloud infrastructure, and data storage, backups, and read-replicas are fully encrypted using the industry standard AES-256 encryption algorithm.
- All servers that provide access to Protected Data are located in the Vendor's virtual private cloud infrastructure and accessible only through load balancers on the boundaries of our private network. No public traffic is allowed on our private networks.
- All access to Vendor resources is password protected using industry best-practices.
- To safeguard participants/registrants against identity theft, every registration through Vendor is followed by an email confirming the transaction.

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

- Families and individuals who use Arbiter Registration 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 Vendor 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 Vendor 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 Participating Educational Agency. 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 Vendor's service shall only include information that is provided by the Participating Educational Agencies. 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 the Vendor 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.

All information provided by families and individuals while using the service are subject to the privacy policy located at <https://hello.familyid.com/privacy-policy> and attached below:

### **Arbiter Registration Privacy Policy**

Your privacy is extremely important to us. This Privacy Policy addresses information collected by ArbiterSports, LLC (“ArbiterSports”, “we” or “us”), and we are committed to respecting your privacy and the confidentiality of your personal data and content. To better protect you, we provide this Privacy Policy to assist you in understanding how we use and safeguard the information you provide in using our online platform (the “Platform”). In this Privacy Policy, our “Product” means the Platform and services, including those provided through our Platform; “Personal Data” means any information that we possess relating to an identified or identifiable user of the Platform, and “Program Provider” means a third party offering a program for which you are submitting information via the Platform. This Privacy Policy is incorporated into, a part of, and governed by our Terms of Service. By using the Arbiter Registration service, you are accepting the terms of this Privacy Policy. If you do not agree to this Privacy Policy, you may not use the Arbiter Registration service.

#### **1. WHAT INFORMATION DO WE COLLECT?**

In order to provide you with use of the Platform, we may gather and process some or all of the following information:

- **Content:** information that is collected from or stored by you on the Platform, other than Account Sign-up Information, Customer Service Communications or Log Information.
- **Account Sign-Up Information:** information provided when you sign up for an account to use the Platform, including, your email address and password.
- **Customer Service Communications:** information that is reported to us about the operation of the Platform.
- **Log Information:** When you use the Platform, our servers automatically record basic information that your application sends in order to access our services. These server logs may include information such as your message, Internet Protocol address, other addressing information, the date and time of your request and an authentication token used to validate the identity of you and your computer.

#### **2. HOW DO WE USE THIS INFORMATION AND FOR WHAT PURPOSE?**

Our primary purpose in collecting information is to provide you with an efficient user experience. Below we describe how we use certain information. We may

use this information to: provide the services and any customer support you request; resolve disputes, collect fees, and troubleshoot problems; enforce our contractual agreements; customize, measure, and improve the Platform; inform you about service updates; compare information for accuracy, and verify your identity; provide other services for you as described when we collect the information. In the future, we may give you the option of using your profile and registration data to enable ArbiterSports to provide you with information on relevant products, services and/or other offers.

### **Account Sign-up Information**

We ask for Account Sign-up Information in order to verify your identity and to enable your use of the Platform.

We respect the privacy of personal e-mail accounts and we will store your e-mail addresses just as securely as other Personal Data. We will not send you unwanted e-mail messages or junk mail, and your details will not be passed to third parties for their marketing purposes without your explicit permission. However, we will use e-mail to send you messages about Platform-related issues. We may also use e-mail to keep you up to date with news about ArbiterSports.

If you do not want to be kept informed in this way by e-mail, please unsubscribe at the bottom of the email message or contact us at [info@familyid.com](mailto:info@familyid.com)

### **Content**

We reserve the right to pre-screen, review, flag, filter, refuse or remove any or all of Content from the Platform.

### **Customer Service Communications**

Information which is voluntarily submitted in feedback is used for the purposes of reviewing this feedback and improving the Platform. We reserve the right to utilize anonymous information for marketing purposes, for instance by displaying selected comments on the Platform or in other communications. Further, we may from time to time ask you to provide information on your experiences which will be used to measure and improve quality. You are at no time under any obligation to provide any of such data. We will never use any personally identifiable (feedback) information without your explicit permission thereto.

### **Log Information**

We will use this routing information to provide you with access to the Platform and for statistical information.

### **Children's Privacy**

We are committed to protecting the privacy needs of children. Accordingly, we do not knowingly collect or solicit personal information

from anyone under the age of 13 or allow such persons to register. No one under age 13 may provide any personal information to the Platform.

### **Student Information**

Individual student data will be managed by ArbiterSports in accordance with the Family Educational Rights and Privacy Act of 1974 (including its implementing regulations, “FERPA”) that govern the confidentiality of, and access to, students’ educational records. ArbiterSports is committed to abide by state and federal laws protecting student data.

### **Requirements of Program Providers**

Program Providers may have specific guidelines and limitations regarding completion and submission of registration forms and use of the information provided. ArbiterSports does not monitor or verify compliance with these requirements or a Program Provider’s use of your information, and you are responsible for all information submitted to a Program Provider.

### **3. TO WHOM DO WE TRANSFER YOUR PERSONAL INFORMATION?**

Except as provided below, we will not sell, rent, trade or otherwise transfer any Registration Information or Content to any third party without your explicit permission, unless we are obliged to do so under applicable laws or by order of the competent authorities.

We may share your information with our affiliates and other service providers (for example, email notification and/or payment processing services as applicable to your registration) which are providing services relating to your use of the Platform. Registration Information that you provide to us may be sent to those providers in order to deliver their services; similarly, personal information that you provide to those providers may be sent to us in order to operate the Platform. Arbiter Registration enables you to submit your personal information to register for programs and activities, among other potential uses. When you elect to submit your personal information to a third party Program Provider or other service, organization, company or individual via the Platform, whether to register for a program or for any other purpose, ArbiterSports is not responsible for how your data is used by that third party. It is solely your responsibility to understand how and with whom that party intends to use and share your personal data. This may include the transfer of your data to other software platforms, sharing of information in the form of reports, or other methods and forms of data sharing and use.

As we continue to develop our business, we might buy or sell subsidiaries or business units. In such transactions as well as in the event all or substantially all of our assets are acquired by a third party, personal information of our users will generally be one of the transferred business assets. We reserve the right to include your personal information, collected as an asset, in any such transfer to a third party. The use of any personal information by a third party transferee shall

continue to be subject to applicable law. In the event of any such transfer, notice will be posted and you may elect to discontinue your use of the Platform and/or request removal of your personal data.

We reserve the right to access, use, preserve or disclose any information we have access to if we have a good faith belief that such access, use, preservation or disclosure is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce our contractual agreements, including investigation of potential violations, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of us, our users or the public as required or permitted by law.

#### 4. HOW DO WE PROTECT YOUR PERSONAL INFORMATION?

We take appropriate organizational and technical measures to protect the information provided to us or collected by us, and we also have protocols in place in the event we identify a security breach. Further, student data housed on the Platform is protected by us and accessible to users in a manner that is consistent with FERPA. You should be aware that internet communications are not always secure. Although we do take what we consider appropriate steps to protect your data, protection of information available over the internet is subject to attack from third parties, and accordingly we cannot guarantee that third parties cannot illegally gain access to Content.

#### 5. HOW LONG IS YOUR PERSONAL DATA KEPT BY US?

We will retain your information for as long as is necessary to: (1) provide the use of the Platform; (2) invoice charges and to maintain records until invoices cannot be lawfully challenged and legal proceedings may no longer be pursued; (3) communicate with you regarding other services that we offer; (4) comply with applicable legislation, regulatory requests and relevant orders from competent courts; (5) enforce our contractual agreements; or (6) fulfill any of the other purposes detailed in this Privacy Policy.

You may request removal of your information at any time. ArbiterSports will delete your information from the Platform within 15 days from the date of your request. Deletion of your data from the Platform will prevent you from accessing your program registration history and details regarding what data you have shared with others through the Platform. The data will be removed from back-ups at the end of the duration of the Arbiter Registration back-up cycle, which is a minimum of 30 days and but is subject to change without notice. Please note that the Program Providers, service providers, individuals, and/or organizations that have received your information will have their own data retention practices and may be subject to regulations that require them to maintain data for a specified period of time. You must contact those entities directly regarding their use and removal of your information.

#### 6. WHAT ARE COOKIES AND HOW DO WE USE THEM?



A cookie is a piece of data stored on the user's hard drive containing information about the user. Usage of a cookie will in no way linked to any personally identifiable information while using the Platform. Once the user closes their browser, the cookie simply terminates. For instance, by setting a cookie on our product, the user would not have to log in a password more than once, thereby saving time while on the Platform. If a user rejects the cookie, they may still use the Platform. The only drawback to this is that the user will be limited. Cookies can also enable us to track to enhance the experience using products, and for analytic purposes to help us understand the use of the Platform.

Some of our business partners may use cookies. However, we have no access to or control over these cookies.

#### 7. HOW FAR DOES OUR RESPONSIBILITY EXTEND?

This Privacy Policy applies to services that are owned and operated by us. We do not exercise control over other users, including Program Providers to whom you submit your information, or third party systems that may use the Platform. They may place their own or other files on their systems, collect data or solicit personal information from you. We accept no responsibility or liability for these other Platforms, Program Providers, or services.

#### 8. CAN THIS PRIVACY POLICY BE MODIFIED?

We reserve the right to modify the provisions of this Privacy Policy from time to time. By using the Platform you consent to this Policy at the time of such use. We recommend that you check this Privacy Policy periodically for any changes. ArbiterSports will provide notice on the platform prior to any material changes to this Policy.

#### 9. WHAT RIGHTS DO YOU HAVE AND HOW CAN YOU CONTACT US?

If you would like to exercise your right to view, correct, complete or remove your Personal Data, please contact us at [info@familyid.com](mailto:info@familyid.com). Upon verification of your identity, we will attempt to quickly fulfill your request, provided we will not act contrary to applicable legislation by fulfilling your request.

- (c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.
- (d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

- (e) Vendor   x   will        will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.
- (g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

Vendor acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the MLSA and the terms of this Data Sharing and Confidentiality Agreement:

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
- (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:
  - (i) the parent or eligible student has provided prior written consent; or
  - (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.
- (h) Promptly reimburse Erie 1 BOCES, another RIC, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

6. **Notification of Breach and Unauthorized Release**

- (a) Vendor shall promptly notify Erie 1 BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or unauthorized release.
- (b) Vendor will provide such notification to Erie 1 BOCES by contacting Michelle Okal-Frink directly by email at mokal@e1b.org, or by calling (716) 821-7200 (office) or (716) 374-5460 (cell).
- (c) Vendor will cooperate with Erie 1 BOCES and provide as much information as possible directly to Michelle Okal-Frink or her designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.
- (d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.
- (e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other RIC or Regional Information Center, or any affected Participating Educational Agency.



Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892

**EXHIBIT D (CONTINUED)**

**PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

- (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.
- (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 for public review at <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or 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, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>.

**BY THE VENDOR:**

*John Hopkins*

**Signature**

John Hopkins

**Printed Name**

CFO

**Title**

5/18/2023

**Date**

## EXHIBIT D (CONTINUED)

### SUPPLEMENTAL INFORMATION

#### ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT BETWEEN ERIE 1 BOCES AND ARBITERSPORTS LLC

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with ArbiterSports LLC which governs the availability to Participating Educational Agencies of the following Product(s):

#### Arbiter Registration

Pursuant to the MLSA, Participating Educational Agencies may provide to Vendor, and Vendor will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law (“Protected Data”).

**Exclusive Purpose for which Protected Data will be Used:** The exclusive purpose for which Vendor is being provided access to Protected Data is to provide Participating Educational Agencies with the functionality of the Product(s) listed above. Vendor agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the MLSA. Protected Data received by Vendor, or any of Vendor’s subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

**Oversight of Subcontractors:** In the event that Vendor engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the MLSA (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Vendor under the MLSA and applicable state and federal law. Vendor will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by:

All ArbiterSports employees and subcontractors who have access to Protected Data managed by our application must complete training on security practices, and agree to follow ArbiterSports’s privacy policies. All Authorized Users are trained to maintain the confidentiality, integrity, availability, and regulatory compliance of non-public information. ArbiterSports tracks the progress of users through the training process to ensure all policies are reviewed and a thorough understanding of the practices that govern compliance are followed.

#### Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on **July 1, 2023** and expires on **June 30, 2026**.

- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.
- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

#### **Duration of MLSA and Protected Data Upon Expiration:**

- The MLSA commences on **July 1, 2023 and expires on June 30, 2026.**
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.
- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

**Challenging Accuracy of Protected Data:** Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or

principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

**Data Storage and Security Protections:** Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

**Encryption of Protected Data:** Vendor (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.