

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 BOCES, 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 BOCES 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:

(c) **OUR PRIVACY POLICY**

GenE is working to provide an esports platform to service scholastic institutions, communities, brands, personalities, and non-profits with the intent to create fair and fun competition for all participants.

By accessing or using our Services, you affirm that you have read and understand this Privacy Policy and expressly consent to our collection, storage, and disclosure of your personal information in accordance with its provisions, as well as our Terms of Use. All capitalized terms used in this Privacy Policy that are not defined herein shall have the meaning given to them in our Terms of Use or other applicable agreements.

We encourage you to familiarize yourself with our privacy practices and contact us with any questions or concerns. If you do not want us to collect and use your personal information as described in this Privacy Policy, it is incumbent upon you to refrain from using our Services.

PERSONAL INFORMATION COLLECTED OR RECEIVED

In the course of providing our Services, we and/or our Partners may collect personal information about you in a few different ways. For instance, we collect personal information during registration, which may vary based on your account type and whether you are a User, Student, School official, Parent, or Team Administrator. Partners, such as the companies that provide games offered, have an agreement with GenE about the security and data privacy of our users.

When registering with us, you are required to choose a password. Other registration information may include the following: name, phone number, email address, School (name, city, state), high school graduation date, age, gender identity, Discord or game ID. We also collect information indirectly from you based on your use of our Services and from our Partners and other third-parties that help us provide Services and with whom you may interact with, such as third party games you access through our Services or third party communities.

Below are some additional details about the information we may collect:

User Registration: GenE collects certain information from all registered users directly including the user's name, email, zip code, phone number, and GamerTag. This information may be shared with third party Communities on our platform when you opt-in to share your information to them directly through the platform.

School or Club Registration and Account Setup: GenE collects certain information when a School official or Team Admin registers a School with GenE, including the official's name, School name, School address, telephone number, School email address, position at School, and information related to the computers, software, hardware, and other IT equipment required for facilitating esports at the School. School officials and Team Admins may also disclose information about Students, such as club

members and team rosters. We may also collect information if a School official corresponds with us via telephone, email, or social media; shares content to our Website or through our Services; or replies to GenE emails or surveys.

Student Registration and Account Setup: GenE may collect information about Students from their School or from the Student directly, including the Student's name, email address, School (name, city, state), and graduation date. We may collect additional optional information associated with the Student's User Profile, including GamerTag, parent/guardian information (name, relation, e-mail, and phone), phone number, grades, gender, photo or avatar, and esports team position. You may directly provide this information to HSEL, or a School official may provide it to us during the team registration process. We refer to personal information collected from or about Students, as well as Student-generated user content, and other information associated with that personal information, as "Student Data."

Parent/Guardian Account Setup: For students under the age of 13 that wish to participate in HSEL Tournaments, a parent or guardian must sign up on their behalf ("Parent Account"). We do not allow Students under the age of 13 to create an account on our platform. HSEL collects certain information about Parents/Guardians, including their name, email, phone, School (name, city, state), and current grade of their participating student. A participating Student's GamerTag may be requested and/or required for participation in specific games. No personally identifying data will be collected on the participating Student when under the age of 13. Parent/Guardian user information and other information associated with this data is referred to as, "Parent Data."

Data Collected Via Service Usage: In order to provide you with our Services, we need to collect, store, and use various information about your activity on our platforms and the use of our Services. For instance, we gather information about your use of the Services, your interaction with the Services, and any content you post to the Services ("User Content"). This User Content may also include win-loss records for Students and School teams; match and tournament statistics; scholarships, awards, and prizes received by Students and/or School Teams; and gameplay highlights featuring Students and/or School teams.

Information Received from Third Parties: We may on occasion obtain personal information about you, including information about Students and Schools from third parties, which is then merged with the information we collect through our Services. For instance, we receive information about your activities from third party game providers you access through our Service. We rely on this information to provide our Services, as well as to enhance their features and functionality. This information all helps us communicate with you, which may include sending you email messages and SMS messages about upcoming matches, allowing you to communicate with other users on

our Services, and disseminating Service-related alerts (e.g., account verification requests, feature updates regarding the Service, and technical /security advisories).

Automated Information: To deliver an individualized user experience and keep our Services secure, we may automatically receive and record certain technical information from your browser or device when you interact with us, such as visiting our various websites, reading our electronic messages, and accessing our Services. We may rely on various tracking technologies, such as cookies, web beacons, file information, and similar technology (collectively, “tracking technologies”), to facilitate data collection.

Tracking technologies collect various types of information, including how you interact with our Services (i.e., the pages you visit and the links you click), your browser and online usage patterns (i.e., the browser you are using and your IP address), the device(s) you use to access the Services (i.e., what type of device you are using and its mobile device identifier), and information about your location (i.e., your IP address may be used to associate your account with your School).

We use tracking technologies for several purposes, such as: streamlining authentication, by remembering your permissions and log-in information; protecting security by detecting software bugs; remembering your user preferences; delivering custom content and information based on how you use the Service; and making improvements to our Service. Additionally, HSEL may collect analytics data, or use third-party analytics tools, such as Google Analytics, to help us gauge Website traffic and Service usage trends. GenE, HSEL and our third-party partners may also use cookies and tracking technologies for advertising purposes.

In most circumstances, you can control the use of cookies by adjusting your browser settings, which may allow you to receive a notification when you receive a cookie, disable existing cookies, or automatically refuse cookies. However, please note that doing so may interfere with your full use of our Services, as some features may not function properly. You may also adjust the settings on your email client to prevent images from being downloaded automatically, which blocks certain technologies that allow us to see whether you have accessed our email, clicked on any links, and performed other functions with it. If you want to opt-out of Google Analytics, you can download and install the [Google Analytics opt-out add-on](#) for your web browser.

DISCLOSURE OF YOUR INFORMATION

We respect your privacy. We don't sell or rent your personal information to third parties for marketing purposes without your express authorization. We may, however, disclose your personal information to our Partners or otherwise when:

- Disclosure is necessary to perform the contractual obligations set forth in our Terms of Use and in order to provide Services to you;
- You have consented to the processing, which can be revoked at any time;

- Disclosure is necessary to comply with a legal obligation, a court order, or to exercise or defend any impending or asserted legal claims;
- Disclosure is necessary to further our legitimate interests, as well as those of our third-party business partners;
- The information is already public; or
- Disclosure is necessary in the public interest, such as to prevent crime or to protect your vital interests or those of others.

More specifically, your information may be shared under the following circumstances:

Public Dissemination of Tournament Data: We post certain information about the results of our tournaments, known as “Tournament Data,” on our Services. This Tournament Data may be visible to other authorized users, website visitors, and the public. Tournament Data includes certain personal information from Player Profiles, including the player’s full name, GamerTag, graduation date, school (name, city, state), photo or avatar, and esports team position, as well as player statistics and gameplay highlights, which will be available publicly on the Service by default when you participate in the Service. Email addresses, parent or guardian information (name, relation, email, and phone), and payment information are not considered Tournament Data and are not available to the general public.

Other Authorized Service Users on The HSEL Platform: We may share personal information with other authorized users of the Service such as club administrators, coaches, and School officials, as well as any school district or state association related to the School’s use of the Service. These users may view a Student’s Player Profile, including email address and, if available, phone number and parent/guardian information.

Game Providers: Third party game providers play a central role in the Services we provide. When you seek to participate in a game provided by a third-party game provider, we disclose your GamerTag ID to that third party game provider to facilitate gameplay on its service. Third party game providers will treat your information in accordance with their own privacy practices, which may differ from those described in our Privacy Policy. You are encouraged to review the privacy policy of any third party game provider before participating in any third party game through the Service.

Affiliated Businesses: We may periodically provide our corporate Partners and official sponsors with information about you, including Student Data, Parent Data and/or User Content as well as information about School officials and other adult users, such as a School name, School official name, and School official email address. Our Partners and sponsors may use this information to offer deals, discounts, and other promotional content to you and or Schools.

Third Party Applications/Services: You may give us permission to share your personal information with third party applications or services that are available (or will be

available) via our Service. For instance, you may authorize us to share your information with recruiters, corporate partners, not-for-profit organizations, and other third parties that are affiliated with us. When we share information with these entities, we will only disclose the information that you have authorized or asked us to share. You can also opt to share content with others by email, SMS message, or by posting content from our Services to social media sites, like Facebook or Twitter. These third parties will treat your information in accordance with their own privacy policies, so we encourage you to review such policies prior to authorizing disclosure of your information.

Our Service Providers: We rely on third-party vendors, contractors, and other service providers to perform services on our behalf, which may include sending emails, processing payments, and providing web hosting and analytic services. These third parties may only use your information to perform these tasks on our behalf and are subject to reasonable confidentiality terms.

Business Reorganization: In the event of a change in ownership, or a merger with, acquisition by, or sale of assets to, another entity, we reserve the right to transfer all of your Personal Information. If the transaction involves the transfer of Student Data, we will require the successor entity to abide by the terms of this Privacy Policy, or we will provide the School with notice and an opportunity to opt-out of the transfer of Student Data by deleting the Student Data prior to the transfer.

Legal and Safety Requirements: We may disclose information with third parties as required by law or subpoena or if we reasonably believe that such action is necessary to (a) comply with the law and the reasonable requests of law enforcement; (b) to enforce our Terms of Use or to protect the security or integrity of our Service; and/or (c) to exercise or protect the rights, property, or personal safety of HSEL, our users, visitors, or others.

Aggregated Information: We may also share information with third parties in an aggregated or otherwise anonymized form that does not reasonably identify you directly as an individual. This aggregate or anonymized data may be used to evaluate and improve our Service, product functionality, and service offerings.

THIRD PARTY TRACKING AND ADVERTISING

We may participate in interest-based advertising and use third party advertising partners to collect information from visitors to the Service for the purpose of displaying interest-based advertisements on other websites, apps or services, social networks, or on other devices you may use. In many cases, these third party ad networks use cookies and tracking technologies to recognize your browser or device and to collect information about your visit to our Service to provide you customized content, advertising, and commercial messages that may be more relevant to your interests, as well as to provide advertising-related services such as reporting, attribution, analytics, and market research.

Please be advised that we will use our best efforts to prevent the use of Student Data for targeted advertising purposes. The steps we take include inhibiting these third party advertising networks from collecting information for targeted advertising purposes when a Student logs into our Services and preventing targeted advertising from being knowingly directed to individuals we know to be Students on our Services or on any other website or online service.

STORING AND SECURING YOUR INFORMATION

Storage and Processing: Your information collected through our Services may be stored and processed in the United States or any other country in which we or our affiliates or service providers maintain facilities. If you are located in the European Union or other regions with laws governing data collection and use that may differ from U.S. law, please note that we may transfer information, including personal information, to a country and jurisdiction that does not have the same data protection laws as your jurisdiction.

Data Security: The security of your information is important to us. We rely on physical, administrative, and technological procedures to assure the security, integrity, and accuracy of all personal information we collect. We conduct periodic risk assessments and work to remediate any identified security and privacy vulnerabilities in a timely manner. We also restrict employee access to personal information to only those who require it to perform their job functions.

We employ industry-standard security measures, such as Secure Socket Layer (SSL) encryption technology, to safeguard information provided to us during the account registration process. Other security safeguards include but are not limited to data encryption, firewalls, and physical access controls to building and files.

Although we make good faith efforts to maintain the security of all Personal Information, and in particular Student Data, we can't guarantee that it will remain free from unauthorized access, use, disclosure, or alteration. In the event that any information under our control is compromised as a result of a breach of security, we will take reasonable steps to promptly investigate the situation. In the event that Student Data is accessed or obtained by an unauthorized individual, we will notify impacted Students and Schools within ten (10) days of the incident, or as otherwise required in compliance with any applicable laws and regulations.

YOUR PRIVACY RIGHTS

State and federal privacy laws provide users with certain rights related to their personal information. Consistent with applicable laws, we give you the option to access, change, and delete certain information, as well as determine how we communicate with you.

Updating or Correcting Account Information: You have the right to request that we rectify inaccurate information about you. You may update your account information by editing your profile or signing into the account settings.

Modifying or Deleting Information: You have the right to request the deletion of your personal information. We may not, however, be able to modify or delete your information in all circumstances. For instance, we may not be able to delete Tournament Data, but we may be able to anonymize certain Tournament Data upon request.

Accessing Your Information: You can access certain personal information associated with your account by visiting your account privacy settings. You can also request a copy of your personal information from us, as well as information explaining how that information is used. If you would like to review your information or have any questions about changing, or deleting your information, please contact us at privacy@highschoolsportsleague.com.

Withdrawing Consent: Where we rely on consent to process your information, you can choose to withdraw your consent at any time using specific features provided to enable you to withdraw consent, such as an email unsubscribe link or your account privacy preferences. By utilizing our Services, to the extent permitted by applicable laws, we will assume you have given your consent to disclose your personal information including, without limitation, Student Data, Parent Data and/or User Content as provided herein.

Objecting to Processing: If we process your information based on our legitimate interests as set forth in this Privacy Policy, or in the public interest, you can object to this processing in certain circumstances. In such cases, we will stop processing your information unless we have compelling legitimate grounds to continue processing or where it is needed for legal reasons.

STUDENT DATA

HSEL collects information about Students who use the Service to compete in esports competitions. As previously described herein, the Student Data we collect through HSEL may include the Student's name, email address, School (name, city, state), and graduation date. Students may also opt to provide additional information in connection with their User Profile, including GamerTag, parent/guardian information (name, relation, e-mail, and phone), grade, phone number, gender, photo or avatar, and esports team position.

HSEL allows Students to save or maintain control over information associated with a Student account by establishing or converting the account to a personal account on the Service or by transferring, sharing or linking such information to a personal account. Information associated with a Student's personal account will not be considered "Student Data."

Please be advised that the Student Data HSEL discloses to third party game providers (e.g., player names or player IDs), as well as any other personal information the game provider collects from the School or its Students directly, is governed by the game provider's own privacy policy and the terms of any other agreement between the game provider and the School. Please review the privacy policy of any third-party game provider to understand their privacy practices before you participate in a third party game.

We understand that Parents and Schools are concerned about the privacy of their Students. We are too. HSEL is committed to the following principles to protect Student Data:

- **Limited Data Collection:** HSEL does not ask Students to divulge more information than is needed to use our Services or which is otherwise required by applicable laws. We also don't share Student Data unless we truly need to do so for our legitimate business purposes or the legitimate business purposes of our Partners, including to maintain, develop, support, or improve our Services, and as otherwise permitted by our Privacy Policy or with the consent of the Parent/guardian, Student or School.
- **No Student Profiling:** HSEL does not create personal profiles of Students other than in furtherance of the School's use of the Service (e.g., Player Profiles and player history are created and displayed as part of the esports tournament statistics and history), or as authorized by a Student or Parent, such as when a student transfers information to a personal account.
- **Strong Data Security:** We maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. In the event that Student Data is accessed or obtained by an unauthorized individual, HSEL will provide prompt notification to all impacted users.
- **Transparency:** We will clearly and conspicuously disclose our data privacy/security policies and practices to our users. In addition, we will not make any material changes to our Privacy Policy or contractual agreements governing the collection or use of Student Data without first notifying the School and providing the opportunity to opt-out before the Student Data is used in a materially different manner than was disclosed when the information was collected.
- **No Data Sales:** We won't sell Student Data unless such sale is made pursuant to a corporate transaction, such as a merger, acquisition, bankruptcy, or other sale of assets. In such transactions, HSEL will require the recipient of any Student Data to abide by the terms of our Privacy Policy, or we will provide the School with notice and an opportunity to opt-out of the transfer of Student Data by deleting the Student Data prior to the transfers.

- **Commitment to Legal Compliance:** HSEL is committed to full compliance with all applicable privacy laws, including the Federal Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. 1232g and 34 CFR Part 99, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232h; the Individuals with Disabilities Education Act ("IDEA").

Use and Disclosure of Student Data: HSEL uses and discloses Student Data in accordance with this Privacy Policy and in accordance with applicable laws.

The type of personal information contained in our Tournament Data may be considered "Directory Data" under FERPA. Accordingly, Schools must confirm that any Tournament Data related to their School and Student esports competitors may be shared publicly through our Services in accordance with your School's definition of Directory Data and/or that you otherwise have a parent or guardian's consent to display such information publicly. If you do not wish to have any Student Data displayed in our Tournament Data, please contact HSEL at privacy@highschoolsportsleague.com to discuss your options.

Retention and Deletion of Student Data: We do not knowingly store Student Data longer than required to provide our Services, unless authorized by a School, Student, or Parent. However, we retain Tournament Data and gameplay statistics, tournament highlights and history indefinitely as part of the official record of the esports competition.

Schools are obligated to keep their Student rosters current and request that HSEL delete or de-identify accounts that the School no longer needs to retain. Unless otherwise directed by a School, Student, Parent, we will delete or de-identify personal information contained in Student accounts in accordance with the terms of any applicable written agreement with the School and our standard data retention schedule.

Schools, Students, and Parents are entitled to delete their accounts at any time by contacting HSEL at privacy@highschoolsportsleague.com. Some data, such as information retained in technical support records, customer service records, backups, and other similar business records, may not be immediately deleted or be able to be deleted completely. HSEL may retain any information that has been de-identified or disassociated with personal identifiers such that the remaining information cannot reasonably be used to identify a particular individual. HSEL will also not delete Student information that has been transferred to a personal account except at the direction of the Student or Parent. Although we may not be able to delete Tournament Data, it may be possible to anonymize certain Tournament Data upon request.

LEGAL COMPLIANCE

Please be advised that our Services may contain links to and from third party websites of our Partners (such as gaming providers), advertisers, social media sites, and other

services. If you follow a link to any of these websites, please note that these websites have their own privacy policies, and we do not accept any responsibility or liability for their privacy policies or content.

HSEL uses Student Data for the sole purpose of providing our Services, in accordance with all relevant contractual agreements. We do not own or control Student Data, which belongs to the Student and/or the School that contracts with HSEL to provide our Services to the Student.

As set forth in our agreements with Schools, our Services are designed to provide protections for Student Data as required by applicable privacy laws, which include:

- ***The Family Educational Rights and Privacy Act (“FERPA”)***: Our Service, along with the data protection policies set forth herein, are designed to satisfy our obligation to protect personal information from Students’ educational records under FERPA. We commit to working with Schools to satisfy all compliance obligations under FERPA.
- ***Children’s Online Privacy Protection Act (“COPPA”)***: HSEL does NOT knowingly collect, use, or share any information from children under the age of 13 without verifiable consent from a parent or guardian. A School may not permit a child under 13 to register for our Service to compete on the School’s esports team, unless the School represents that it has the authority to provide all required consents for HSEL to collect and use such Student’s personal information in the manner contemplated by this Privacy Policy and as permitted by COPPA. Please contact us at privacy@highschoolsportsleague.com if you believe we have inadvertently collected personal information of a child under 13 without proper consent so that we may delete such data as soon as possible.
- ***Students Online Personal Information Protection Act (“SOPIPA”)***: This Privacy Policy and our Services are designed to comply with SOPIPA. HSEL does not use Student Data for targeted advertising purposes. We also do not use the information we collect to create a Student profile except in furtherance of providing the features and functions of the Service. We never sell Student Data unless the sale is made in conjunction with corporate transaction, such as a merger, acquisition, bankruptcy, or other sale of assets, in which case we will make efforts to ensure the successor entity honors this Privacy Policy and/or we will notify the School and provide an opportunity to opt-out by deleting Student accounts prior to the data transfer.
- ***California Assembly Bill 1584 (“AB 1584”)***: This Privacy Policy and our Services are designed to comply with AB 1584. Pupil records obtained by HSEL from a local educational agency (“LEA”) remain the property of and under the control of the LEA. Parents, legal guardians, or eligible pupils may review personally identifiable information in the pupil’s records and correct any errors by contacting their LEA directly. In the event of an unauthorized disclosure of a pupil’s records, HSEL will notify the LEA and will provide the LEA with

information to be shared with the affected parent(s), legal guardians(s), or eligible pupil(s). Pupil records will be deleted and/or de-identified in accordance with our agreements with each School and as described in this Privacy Policy.

- **Connecticut Act Concerning Student Data Privacy:** In compliance with the requirements of the Connecticut Act Concerning Student Data Privacy, Conn. Gen. Stat. Ann. § 10-234aa-dd, HSEL has developed a terms-of-service addendum. Please contact us at privacy@highschoolsportsleague.com to find out about incorporating the Connecticut Addendum into your agreement with HSEL.

YOUR CALIFORNIA PRIVACY RIGHTS

California's "Shine the Light" law (Civil Code Section §1798.83) entitles California residents that have an established business relationship with us to request certain information regarding personal information disclosed to third parties for their direct marketing purposes during the immediately preceding calendar year. To make such a request, please contact us at privacy@highschoolsportsleague.com.

The California Consumer Privacy Act ("CCPA") also provides users with additional rights related to their personal information. Consistent with the CCPA, and as set forth in this Privacy Policy, HSEL gives you the choice of accessing, editing or deleting certain information, as well as choices about how we contact you.

In accordance with the CCPA, California residents may request disclosure of the specific pieces and/or categories of personal information that HSEL has collected about them, the categories of sources for that personal information, the business or commercial purposes for collecting the information, the categories of personal information that we have disclosed, and the categories of third parties with which the information was shared.

HSEL does not sell personal information to third parties for monetary value. However, to the extent that HSEL's data processing is construed to involve the "sale" of personal information (as that term is broadly defined under the CCPA), California residents are entitled to opt-out of the "sale" of data at any time.

Although we do our best to honor the privacy preferences of our visitors, we are not able to respond to Do Not Track signals from your browser at this time.

CONTACT US

If you have any questions about this Privacy Policy or our Services, please contact us at privacy@highschoolsportsleague.com or by writing to us at High School Esports League, Inc, 908 Baltimore Ave, Kansas City, MO 64105, Attention: GenE Legal Department.

Additionally, if you have a disability and would like to access this Privacy Policy in an alternative format, please let us know using the contact information above.

PRIVACY POLICY CHANGES

As we are constantly improving our Services and expanding our business. We reserve the right to periodically modify or update this Privacy Policy. If we modify our Privacy Policy in a material manner, such as seeking to use your information in a significantly different way than we previously disclosed, we will notify you by sending a notice to the primary email address associated with your account.

When we make any changes to this Privacy Policy, we will update the “last modified” date at the top of this page. If you object to our changes, you may terminate your GenE account and/or discontinue use of our Services. Continuing to use our Services after we publish changes to this Privacy Policy means that you consent to the changes.

- (d) Vendor will comply with all obligations set forth in Erie 1 BOCES’ “Supplemental Information about the MLSA” below.
- (e) 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.
- (f) Vendor _____ will X 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.
- (g) 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.
- (h) 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 BOCES, 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 BOCES or Regional Information Center, or any affected Participating Educational Agency.

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:

Jordan Mask
53800592CF99454...

Signature

Jordan Mask

Printed Name

Account & Finance Manager

Title

5/9/2023

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT

BETWEEN

ERIE 1 BOCES AND HIGH SCHOOL E-SPORTS LEAGUE, INC.

Erie 1 BOCES has entered into a Master License and Service Agreement (“MLSA”) with HIGH SCHOOL E-SPORTS LEAGUE, INC. which governs the availability to Participating Educational Agencies of the following Product(s):

High School Esports League and Middle School Esports League tournaments and tournament services and the *Gaming Concepts* educational resources

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: N/A

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.