Address: 355 Harlem Rd

West Seneca, NY 14224

Address: 1501 Broadway Time Square, 12th Floor, New York, NY 10036

Date: 5/16/2023

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 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: Kinems uses servers hosted in Microsoft's Azure Cloud Computing Platform

in the East US data center (Virginia). Microsoft uses industry standard access mechanisms to protect Windows Azure's physical infrastructure and datacenter facilities. Access is limited to a very small number of operations personnel, who must regularly change their administrative access credentials. Datacenter access, and the authority to approve data center access, is controlled by Microsoft operations personnel in alignment with local data center security practices. Data are protected and encrypted. Protected Data is encrypted using AES-256 before being stored in the Company's databases. Account credentials are encrypted using bcrypt before being stored in the Company's databases. The Company's web services use HTTPS with TLS certificates to encrypt and secure all the web traffic that is exchanged, and downloads such as pdf reports are generated on demand and not stored on the server.

(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 [*check one*] _____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.

(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 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)

KINEMS DATA HANDLING POLICY

Last updated: September 1, 2019

Kinems, Inc. ("We") take the protection of our customers' data and information, particularly data related to student users of our platform, very seriously. The purpose of this Data Handling and Privacy Statement is to inform our customers about our current data security policies and practices regarding student data, which are intended to safeguard this sensitive information. We handle customer data in a manner consistent with applicable laws and regulations, including, without limitation, the Federal Family Educational Rights and Privacy Act (FERPA), and other state student data privacy protection laws.

This policy covers the collection, use and storage of student data that is obtained through the use of Kinems learning games platform and related services provided by Kinems, Inc. For more information on the collection, use and storage of other data by Kinems, please see our privacy policy, which is incorporated herein by reference.

We receive certain information from each school district customer to enable teachers (as used herein, "teachers" includes school administrators and staff) and students to use Kinems learning games. The following information is generally provided to Kinems, Inc for each student and teacher user of Kinems learning games: student full name or nickname, student grade level, teacher name and teacher e-mail. When students use Kinems learning games certain performance results and usage metrics are also created. These results and usage metrics are used by Kinems, Inc as described below. While teachers and school administrators are able to access student information and the related usage data, this information is not made available to other students, other teachers not related to the students or the public. Each teacher's access is limited only to their students' data. Note that Kinems, Inc does not collect personally identifiable information directly from students. All student information is provided by school district customers or created through the use of the platform.

Please note that Kinems does not collect, obtain, or retain information from any individual on the political affiliation, voting history, religious affiliation, or biometric information (including but not limited to information collected from the electronic measurement or evaluation of any physical or behavioral characteristics that are attributable to a single person, including fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other physical characteristics used for the purpose of electronically identifying that person with a high degree of certainty).

Kinems, Inc only uses student data for education related purposes. Kinems, Inc, only uses student and teacher identifiable data provided by schools and/or school districts to make Kinems learning games available to that particular student or teacher, to provide related reports and

services to that student's school and school district and its teachers and administrators. Kinems, Inc uses student data collected from the use of the Kinems learning games for the purpose of making our service available to its customers. Kinems Inc, collects and uses aggregated, de-identified student data for core product functionality to make Kinems learning games a more effective, adaptive product. "De-identified student data" refers to data generated from usage of Kinems learning games from which all personally identifiable information has been removed or obscured so that it does not identify individual students and there is no reasonable basis to believe that the information can be used to identify individual students. Kinems, Inc does not attempt to re-identify de-identified student data and takes reasonable measures to protect against the re-identification of its de-identified student data. Kinems, Inc does not sell student data or otherwise share student identifiable data with third parties. Kinems, Inc does not include advertisements within Kinems learning games nor does it use student data for targeted advertising in any manner.

Kinems learning games is a cloud-based standalone application. Our servers are located in Tier 4 data centers located in the United States. We do not store any data outside of the US.

Kinems Inc, systems and servers are hosted in a cloud environment. Our hosting provider (Microsoft Azure) implements network-level security measures in accordance with industry standards. In addition, Kinems, Inc manages its own controls of the network environment.

Access to production servers is limited to a small, identified group of operations engineers that are trained specifically for those responsibilities. The servers are configured to conduct daily updates for any security patches that are released and applicable. The servers have anti-virus, intrusion detection, configuration control, monitoring/alerting and automated backups. In addition, Kinems, Inc conducts regular vulnerability testing.

Kinems, Inc employs experienced IT staff that manages and secures its corporate and employee IT systems. Laptops are centrally managed with respect to configuration updates and anti-virus. Access to all Kinems, Inc computers and laptops is password-controlled. Kinems, Inc sets up teacher and administrator accounts for Kinems learning games so that they are also password-controlled.

Kinems learning games is only accessible via https and all public network traffic is encrypted with the latest encryption standards. Encryption of data at rest is implemented for all data stored in the Kinems learning games system.

Kinems, Inc limits access to personal information we have collected to those employees and agents who need to have such access in order to allow Kinems, Inc to provide quality products and services to its customers. Kinems, Inc requires all employees and agents who have access to Kinems, Inc servers and systems to sign non-disclosure agreements. Kinems, Inc requires its employees and contractors who have access to student data to participate in annual training sessions on IT security policies and best practices. Any employee who ceases working with

Kinems, Inc is reminded of his or her non-disclosure obligations at the time of departure, and network access is terminated at that time.

Personal information stored by Kinems is used only in the production systems and only for provision of the explicitly identified functions of the Kinems learning games application. Upon the written request of a customer, Kinems, Inc will remove all personally identifiable student and teacher data related to such customer from its production systems at the end or during the contract. In addition, Kinems, Inc, reserves the right, in its sole discretion, to remove a particular customer's data from its production servers within a reasonable period of time after its relationship with the customer has ended, as demonstrated by the end of contract term or a significant period of inactivity in all customer accounts. Personal information is removed from backups in accordance with Kinems', Inc data retention practices. If Kinems, Inc is required to restore any materials from its backups, it will purge all personal information not currently in use in the production systems from the restored backups.

Teachers or parents of students who use Kinems learning games may request access to or removal of their child's personally identifiable data from Kinems learning games by contacting their students' teacher or school administrator. The teacher or school administrator can then verify the identity of the requesting party and notify Kinems, Inc of the request. Kinems, Inc will promptly comply with valid requests for correction or removal of student data; however, removal of student personally identifiable data will limit that student's ability to use Kinems learning games platform.

Kinems, Inc follows documented "Security Incident Management Procedures" when investigating any potential security incident. In the event of a data security breach, Kinems, Inc will notify impacted customers as promptly as possible that a breach has occurred, and will inform them (to the extent known) what data has been compromised. Kinems, Inc expects customers to notify individual teachers and parents of any such breach to the extent required, but will provide customers reasonably requested assistance with such notifications.

KINEMS PRIVACY POLICY

Last updated: September 1, 2019

Kinems, Inc. ("Kinems") offers a platform of movement-based educational games for use in special education (the "Platform"), which provide real-time body performance visualizations and learning analytics for monitoring students' progress. Kinems respects the privacy of every individual and takes precautions to maintain individual privacy.

- We are committed to providing a secure environment for our services.
- We use the information provided to us to enable the use of and improve our services,

provide

- users with customer service, and authenticate website visits and usage.
- All information collected by Kinems is stored on secure servers.
- Kinems does not sell, lease, or rent personal information without your explicit consent.

This privacy policy is designed to inform users of Kinems at its website available at kinems.com (the "Site") and its Platform (the Site and the Platform, collectively, the "Service") about how we gather and use personal information collected by us in connection with use of the Service. We will take reasonable steps to protect user privacy consistent with the guidelines set forth in this policy and with applicable U.S. state and federal laws, including without limitation, the Federal Family Educational Rights and Privacy Act (FERPA) and other state student data privacy laws.

We take these precautions in an effort to protect your information against security breaches. However, this is not a guarantee that such information may not be accessed, disclosed, altered, or destroyed by breach of such firewalls and secure server software. By using our Site, you acknowledge that you understand and agree to assume these risks.

In this policy, "user" or "you" means any individual or enterprise using the Service, whether as the customer purchasing the Service or an authorized user of the Service.

BY ACCESSING OR USING THE SERVICE, YOU ACKNOWLEDGE THAT YOU HAVE READ, UNDERSTAND, AND AGREE TO BE BOUND BY THIS PRIVACY POLICY. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT USE THE SERVICE.

Personal Information: We collect the following personal information about you in connection with the Service: (a) when you register to use the Service as a customer, through a trial or standard account, or use the Service as a teacher or administrator of a school customer, we will collect your first name, last name, e-mail address (b) if you communicate with us by email but do not otherwise register to use the Service, we will collect your email address; and (c) if you communicate with us through our chat module or contact form, we collect the information that you provide to us. All of this information is referred to in this Policy as "Personal Information".

Please note that Kinems does not collect, obtain, or retain information from any individual on the political affiliation, voting history, religious affiliation, or biometric information (including but not limited to information collected from the electronic measurement or evaluation of any physical or behavioral characteristics that are attributable to a single person, including fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other physical characteristics used for the purpose of electronically identifying that person with a high degree of certainty).

School District Customers. When school districts use the Service, we collect certain information from the school districts for each student and teacher user of the Service, to enable students and teachers to use the Service, including: student name(s) or nickname(s), student grade level(s), teacher name(s) and teacher e-mail address(es). We also collect performance results and usage metrics generated from students' use of the Service. Only school administrators and teachers can access student information and metrics, and teachers can only access information related to their students. We do not collect Personal Information directly from students.

Use of Anonymous Information. We may use Anonymous Information (as defined below), or disclose it to third party service providers, to provide and improve the Service. "Anonymous Information" means information which does not enable identification of an individual user, such as aggregated information about use of the Service.

Web Tracking Information: We, and our third party service providers, may use web tracking technologies such as cookies, pixel tags and clear GIFs in order to operate the Service efficiently and to collect data related to usage of the Service. Such collected data ("Web Tracking Information") may include the address of the websites you visited before and after you visited the Service, the type of browser you are using, your Internet Protocol (IP) address, what pages in the Service you visit and what links you clicked on, and whether you opened email communications we send to you. In order to collect Web Tracking Information and to make your use of the Service more efficient, we may store cookies on your computer. We may also use web tracking technologies that are placed in web pages on the Service or in email communications to collect information about actions that users take when they interact with the Service or such email communications. We do not correlate Web Tracking Information to individual user Personal Information. Some Web Tracking Information may include data, such as IP address data, that is unique to you. You may be able to modify your browser settings to alter which web tracking technologies are permitted when you use the Service, but this may affect the performance of the Service.

Log Files. When users visit our Site, Kinems gathers certain information automatically and stores it in log files. This information includes Internet Protocol (IP) addresses, browser type, Internet Service Provider, referring/exit pages, operating system, and date/time stamp. We use this information to monitor the usage of our Site. Also, when we send e-mails to you, we may be able to identify information about your email address, such as whether you can read graphic-rich HTML emails. We use this information not to identify individual users, but to analyze trends, administer the Site, track users' movements around the Site, and gather demographic information about our user base as a whole which provides us with the ability to determine aggregate information about our user base and usage patterns. We may, in some circumstances, need to review this automatically collected data in combination with specific registration information to identify and resolve issues for individual users.

Cookies. The Kinems Site also uses cookies to enhance the browsing experience on the Site. A cookie is a small text file or record that is stored on a user's computer when you visit the Site, which collects information about your activities on the Site. The cookies transmit this

information back to the computers at Kinems; these computers are, generally speaking, the only computers which are authorized to read such information. The information captured makes it possible for us to: (i) speed navigation, and provide you with custom tailored content; (ii) remember information you give to us, so you don't have to reenter it each time you visit the Site; and (iii) monitor total number of visitors to the Site and pages viewed. You can choose to have your browser warn you every time a cookie is being sent to you or you can turn off cookie placement. By not using cookies, your overall internet browsing experience will be affected.

User Data: "User Data" is that data -- other than Personal Information -- that school districts provide us regarding or related to their students who are using the Kinems Platform. We store User Data in order to provide the Service.

Personal Information Generally: We will use and store your Personal Information for the purpose of delivering the Service, and to analyze and enhance the operation of the Service. We may also use your Personal Information for the internal operational and administrative purposes of the Service.

Personal Information from Schools: We only use Personal Information of students and teachers that has been provided to us by our school customers to make the Service available to those students or teachers, and to provide related reports to the applicable school district, teachers and administrators, and to improve the content and effectiveness of the Service.

Web Tracking Information: We use Web Tracking Information to administer the Service and to understand how well our Service is working, to store your user preferences, and to develop statistical information on usage of the Services. This allows us to determine which features best to help us improve our Service, to personalize your user experience, and to measure overall effectiveness.

Aggregate and De-Identified Information Generally: We will also create statistical, aggregated and/or de-identified data relating to our users and the Service for analytical purposes. Aggregated and/or de- identified data is derived from Personal Information and User Data but in its aggregated and/or de- identified form, it does not duplicate or reveal any User Data or relate to or identify any individual. This data is used to understand our customer base and to develop, improve and market our services. Aggregate and De-Identified Information from Schools: We use aggregated, de-identified student data for core product functionality and to improve the Services. We do not attempt to re-identify de- identified student data and take reasonable measures to protect against the re-identification of its de- identified student data.

Customer Testimonials: We may post customer testimonials on our Site, and may use testimonials in other formats consistent with consent received. Customer testimonials may contain personally identifiable information. We may use your Personal Information to contact you to obtain a testimonial and obtain your consent via email or agreement sent via fax, pdf or mail prior to using such testimonial and/or using your name along with your testimonial.

Legal Exception: Notwithstanding the above, we may in any event store and use Personal Information and User Data to the extent required by law or legal process, to resolve disputes, to enforce our agreements (including this Privacy Policy) with you, or if in our reasonable discretion use is necessary to protect our legal rights or to protect third parties.

Email Communications: If you register and provide your email address, we will send you administrative and promotional emails. If you wish to opt out of promotional emails, you may do so by following the "unsubscribe" instructions in the email, or by editing your account settings as described below. All users receive administrative emails, and so you cannot opt out of them while you remain registered.

Personal Information and User Data: We will not disclose your Personal Information or User Data to any third parties except as follows:

1. to third party contractors engaged to provide services on our behalf ("Contractors"), such as performing marketing, analyzing data and usage of the Service, hosting and operating the Service or providing support and maintenance services for the Service, or providing customer service. We enter into agreements with all Contractors that require Contractors to use the Personal Information they receive only to perform services for us.
2. for school customers, we disclose Personal Information and User data of students and teachers using the Service to applicable teachers and administrators, solely to provide the Services to those students and teachers. We do not display advertisements within the Service, nor do we disclose student information for any advertising purpose.

3. when we have your consent to share the information.

Web Tracking Information: We disclose Web Tracking Information to Contractors, in order to analyze the performance of the Service and the behavior of users, and to operate and improve the Service.

Aggregate Information: We may disclose aggregated data that does not contain Personal Information or User Data to third parties, such as potential customers, business partners, and funding sources, in order to describe our business and operations.

Network Operators: Use of the Service may involve use of the services of third party telecommunications carriers. Such carriers are not our contractors, and any information that a carrier collects in connection with your use of the Service is not "Personal Information" and is not subject to this Privacy Policy. We are not responsible for the acts or omissions of telecommunications carriers.

Additional Disclosures: We reserve the right to disclose any information we collect in connection with the Service, including Personal Information, to: (a) any successor to our business as a result of any merger, acquisition, asset sale or similar transaction; and (b) any law enforcement, judicial authority, or governmental or regulatory authority, to the extent required

by law or if in our reasonable discretion disclosure is necessary to enforce or protect our legal rights or to protect third parties.

Upon the written request of a school customer or within a reasonable amount of time after (a) the termination of a customer's contract with us or (b) inactivity of a customer in using the Service, we will remove all Personal Information related to students, teachers and administrators associated with such customer. We remove backed-up data in accordance with our standard data retention practices. In the event we are required to restore backed-up data, we will purge all Personal Information not currently in use from the restored back-ups. We will remove or correct Personal Information of students whose schools are our customers at the request of their parents, teachers or school administrators; removal will, however, limit students' ability to use the Service.

If you would like your Personal Information permanently removed from our database, please contact us at privacy@kinems.com. We will promptly delete your Personal Information and you will no longer receive email from Kinems. Your removal from the mailing list or database will not remove data you have submitted to us or records of past use of the Service, nor delete information stored in our data backups and archives. Such data will be maintained and/or deleted in the ordinary course of Kinems' business.

California Online Privacy Protection Act Notice

On September 27, 2013, California enacted A.B. 370, amending the California Online Privacy Protection Act to require website operators like us to disclose how we respond to "Do Not Track Signals"; and whether third parties collect personally identifiable information about users when they visit us.

(1) We do not track users who do not interact with our sharing functionality across the web, and therefore do not use "do not track" signals.

(2) We do not authorize the collection of personally identifiable information from our users for third party use through advertising technologies without separate member consent.

California Civil Code Section 1798.83 also permits our customers who are California residents to request certain information regarding our disclosure of Personal Information to third parties for their direct marketing purposes. To make such a request, please send an email to privacy@kinems.com. Please note that we are only required to respond to one request per customer each year.

Security: We use reasonable security precautions to protect the security and integrity of your Personal Information in accordance with this policy and applicable law. The Service is hosted in a cloud environment and the hosting provider implements network-level security measures in accordance with industry standards. However, no internet transmission is completely secure, and we cannot guarantee that security breaches will not occur. Without limitation of the foregoing,

we are not responsible for the actions of hackers and other unauthorized third parties that breach our reasonable security procedures.

Links: The Kinems Service may contain links to other websites. Kinems is not responsible for the privacy practices or the content of those websites. Users should be aware of this when they leave our Site and review the privacy statements of each third party website. This Privacy Policy applies solely to information collected by the Service. We encourage our users to read the privacy policies of these other web sites before proceeding to use them.

Amendments: Kinems may modify or amend this policy from time to time. If we make any material changes, as determined by Kinems, in the way in which Personal Information is collected, used or transferred, we will notify you of these changes by email and by posting a modified version of this Privacy Policy on our website. Notwithstanding any modifications we may make, any Personal Information collected by Kinems from you will be treated in accordance with the privacy policy in effect at the time information was collected, unless we obtain your consent otherwise.

Children: Kinems does not knowingly collect or maintain personally identifiable information from persons under 13 years of age without obtaining verifiable prior consent from parents or, if permitted by applicable law, schools acting on behalf of parents, and no part of the Service is directed to be used by persons under 18 without verifiable consent by or on behalf of their parents. If you are under 18 years of age, then please do not use the Service other than under the direction of your parent, guardian, or school acting on their behalf. If Kinems learns that personally identifiable information of persons less than 13 years of age has been collected without the appropriate consent, then Kinems will take the appropriate steps to delete this information. To make such a request, please contact us at privacy@kinems.com.

Service Visitors from outside the United States: Kinems is a cloud-based standalone application and its servers are located in the United States and are subject to the applicable state and federal laws of the United States. If you choose to access or use the Service, you consent to the use and disclosure of information in accordance with this privacy policy and subject to such laws. For users outside the United States, please note that any data or personal information you provide to the services or Site will be transferred out of your country and into the United States. You warrant that you have the right to transfer such information outside your country and into the United States.

Effective Date of this Policy: September 1, 2019

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:

DocuSigned by:
Michail Boloudakis
023F62D29334410...
Signature

Michail Boloudakis
Printed Name

CEO
Title

5/16/2023

Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND KINEMS INC.

Erie 1 BOCES has entered into a Master License and Service Agreement ("MLSA") with Kinems Inc. which governs the availability to Participating Educational Agencies of the following Product(s):

Kinems learning games

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: NA

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.