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, but that adoption may not occur until a date subsequent to the effective date of the MLSA. Erie 1 BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption., and 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: Gizmos and Reflex are on servers and equipment owned and operated by its parent company Cambium Learning. Our servers and all user-specific data are hosted

in a secure Tier 4 enterprise data center located in Texas with a failover data center in Michigan. All of our administrative controls are behind firewalls and also require username/password access, which is limited to Cambium Learning operational staff. *Science4Us* data is stored in our databases, which are maintained in dedicated, secure servers hosted in the Microsoft Azure Cloud. We have provided a copy of Data Security and Privacy Plan in a separate document.

ExploreLearning is committed to protecting your online privacy. Our programs are certified COPPA, FERPA & CSPC compliant.

Security Safeguards
We are committed to protecting student data against unauthorized access, destruction, use, modification or disclosure. Protecting student data requires efforts from us and from you. We will implement reasonable and appropriate safeguards when collecting student data from you and when storing that student data in our database and you will observe our security safeguards and exercise reasonable caution when using this site.

Specific institutional and technological security safeguards include:
1. Only ExploreLearning employees who are authorized to handle student data are able to access the Data Management System.

2. Only school district employees and representatives that the district authorizes as school officials are permitted to access the system. It has a hierarchical permissions system. This means:

1. A teacher will only be able to see data for his/her class.

2. A Principal, Coach, or other authorized School User will be able to view all data at a given school.

3. An authorized district-level employee, such as an Instructional Coordinator or Superintendent, will be able to see all data across the district.

3. Each authorized school official is given a User ID and Password valid only for the duration of the academic year, including a summer program if applicable. You must safeguard your User ID and Password, and not permit any unauthorized access to student data entered or kept in ExploreLearning's system.

4. Upon written request by the district, ExploreLearning will destroy any student data for districts who no longer participate in an ExploreLearning program. ExploreLearning will provide written verification that the data has been destroyed as requested.

5. If a district has not used any ExploreLearning product for a period of two years, ExploreLearning will provide written notice that the student data pertaining to their district will be destroyed, unless the district requests the records be kept. Upon destruction, ExploreLearning will provide written verification that the data has been destroyed.

6. ExploreLearning uses industry standard server and network hardware and software to ensure that data is protected from unauthorized access or disclosure.

Although we make concerted good faith efforts to maintain the security of personal information, and we work hard to ensure the integrity and security of our systems, no practices are 100% immune, and we can't guarantee the security of information. Outages, attacks, human error, system failure, unauthorized use or other factors may compromise the security of user information at any time. If we learn of a security breach or other unauthorized disclosure of your Personally Identifiable Information (PII), we will attempt to notify you so that you can take appropriate protective steps by posting a notice on our homepage (www.explorelearning.com) or elsewhere in our Service and we will send email to you at the email address you have provided to us. Additionally, we will notify the primary administrative contact at your school or district by email and telephone and assist with their efforts to ensure your notification.

Any such notice will include:

- The date of the breach.
- The type of information that was subject to breach.
- General description of what occurred.
- Steps we are taking to address the breach.
- The contact person with our Company who you can contact regarding the breach.

If you are a parent, legal guardian or eligible student and an unauthorized disclosure of your student's PII records occurs, we will notify you by email at the email address we have on record for you or through notice to your school or district's primary administrative contact in the event that we do not have an email address on record for you.

When you use this site, you consent to our privacy practices and agree to accept the responsibilities **outlined in this statement.**

(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 subcontactors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontactors, 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)

ERIE 1 BOCES

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

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:

Signature

Amy Otis
Printed Name

Vice President, Bids and Contracts
Title

05/26/2020
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND EXPLORELEARNING, LLC

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

Gizmos, Reflex, and Science4Us

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 subcontactors, 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 subcontactors, 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 subcontactors, assignees, or other authorized agents abide by the provisions of these agreements by: N/A, ExploreLearning will not utilize subcontractors, as well subcontractors do not have access to school or student data.

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on [May 26, 2020] and expires on [June 30, 2023].
- 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.

ExploreLearning

ExploreLearning is committed to protecting your online privacy. Our programs are certified COPPA, FERPA & CSPC compliant.

Data Security and Privacy Policies can be found online.

Science4Us: https://www.science4us.com/privacy-policy/
Gizmos: www.explorelearning.com/privacy
Reflex: https://accounts.explorelearning.com/reflex/privacy

Science4Us

This provides you with access to ExploreLearning's Data Management System. This system is an integral component of ExploreLearning's curriculum products and provides valuable reporting, instructional recommendations, and other resources used by teachers and other instructional leaders in conjunction with ExploreLearning's curriculum with the goal of improving student performance.

This statement describes the privacy and security practices ExploreLearning employs for this site. We have adopted these practices to protect you, the students, and the school district, and to enable each of us to comply with applicable legal requirements. Use of this site requires district acceptance of the practices outlined in this statement.

Two types of personally identifiable information are used on this site: **your personal data** and **student data**.

Your Personal Data

Collection

ExploreLearning collects information from you as you use this site. For example, you must enter certain personally identifiable information, including your name, e-mail address, and phone number. We use this information to verify your identity and prevent unauthorized access to your account and to contact you in connection with your use of this site.

In addition to the information you provide, ExploreLearning collects information about your use of this site through tracking, cookies, and log files, as described in our general Terms of Use statement.

Protection

Because you enter your personal data, you control its accuracy. If you discover that your personal data is inaccurate or if it changes or if you want to retain possession of it, you may make corrections by notifying us at support@ExploreLearning.com or call 888-399-1995. We will not share your personal data collected through this site with third persons without your consent. However, your personal data will be available to authorized users from your school district who have permission from the school district to access it. We will not use your personal data collected through this site for any purpose other than providing you with access to this site and the associated services. We will use the same security to protect your personal data that we use to protect student data collected through this site.

Student Data

As you use this site, you will enter student data or interact with student data that has already been entered. Federal law (the Family Educational Rights and Privacy Act, "FERPA") allows a school district to release student records to an organization that is "conducting studies for, or on behalf of, educational

agencies or institutions for the purpose of developing, validating, or administering predictive tests... [or] improving instruction."

However, FERPA requires limitations on disclosure of those records and implementation of appropriate security measures to protect those records. To help your school district comply with FERPA, ExploreLearning has adopted certain practices, and requires that educators using this site fulfill certain responsibilities to safeguard student data. Additionally, ExploreLearning operates in compliance with the Children's Online Privacy Protection Act ("COPPA") and obtains consent when necessary to collect information from children under 13 years of age.

The following statement explains our practices and your responsibilities regarding the student data you enter on this site.

Student Data Security and Confidentiality Statement

Purposes of Data Entry

You control what student data is entered on this site and you retain ownership of the student data at all times. Student data entered on this site should be limited to information that is relevant to the legitimate educational purpose of improving student performance. We will not ask you to enter, and you are instructed not to enter, data about students that is not relevant to this legitimate educational purpose.

Therefore, only a minimum amount of personally identifiable student data required for the setup of the system is requested. We require student first name, student last name, and student identification number. Additional data, not specific to the student, is also required to complete system setup, including the teacher's first and last name, class name, grade level, and school name. Student demographic data, for the purposes of optional disaggregated reporting, is requested separately from the initial setup data and is obtained only with written permission from your district.

Use, Disclosure, and Storage

We will use the student data to provide the services to your school district. We will not keep the student data after you or the school district instructs us to delete it. You may not disclose or otherwise use the student data entered on this site for any unauthorized purposes.

We will only disclose student data to authorized employees or representatives of the school district, and will not knowingly disclose the student data to any third person without express written authorization. When, at the request of the district, we acquire assessment or other information, including personally identifiable student data, from a third party source we treat that information with the same confidentiality and security safeguards as though it were provided directly by the district. Additional agreements may be required by the third party to authorize transmission of data to ExploreLearning.

Your district may from time to time request that ExploreLearning provide student data to third parties of its choosing. We will do so with written authorization, which acknowledges that ExploreLearning is providing that data as your district's agent and that once the data is received by the third party, ExploreLearning no longer has any control over the use or disposition of the data.

We may also use aggregated data in our research, product development, and marketing. That aggregated, non-personally identifiable data (e.g., summary or statistical data) may be shared with third parties. However, we do not use personally identifiable student data to market any products or services directly to students or their parents.

In the event that ExploreLearning wishes, from time to time, to release aggregated data that identifies your school or school district by name, ExploreLearning will enter into a separate agreement with you to authorize release and publication.

ExploreLearning

ExploreLearning does not utilize third parties to provide products and does not share your student data with any third parties.

We may sell, transfer or otherwise share some or all of our assets, including your Personal Information, in connection with a merger, acquisition, reorganization or sale of assets or in the event of bankruptcy. Your consent to this Privacy Policy followed by your submission of Personal Information represents your explicit agreement to that transfer.

Data Quality

You are responsible for keeping the student data that you enter accurate, complete and up-to-date. If you recognize that student data is inaccurate, incomplete, or out-of-date, you are responsible for correcting it. If you experience problems making corrections to student data, please notify us at support@ExploreLearning.com and we will assist you with making corrections.

Security Safeguards

We are committed to protecting student data against unauthorized access, destruction, use, modification or disclosure. Protecting student data requires efforts from us and from you. We will implement reasonable and appropriate safeguards when collecting student data from you and when storing that student data in our database and you will observe our security safeguards and exercise reasonable caution when using this site.

Specific institutional and technological security safeguards include:

1. Only ExploreLearning employees who are authorized to handle student data are able to access the Data Management System.
2. Only school district employees and representatives that the district authorizes as school officials are permitted to access the system. It has a hierarchical permissions system.
   This means:
   1. A teacher will only be able to see data for his/her class.
   2. A Principal, Coach, or other authorized School User will be able to view all data at a given school.
   3. An authorized district-level employee, such as an Instructional Coordinator or Superintendent, will be able to see all data across the district.
3. Each authorized school official is given a User ID and Password valid only for the duration of the academic year, including a summer program if applicable. You must safeguard your User ID and Password, and not permit any unauthorized access to student data entered or kept in ExploreLearning's system.
4. Upon written request by the district, ExploreLearning will destroy any student data for districts who no longer participate in an ExploreLearning program. ExploreLearning will provide written verification that the data has been destroyed as requested.
5. If a district has not used any ExploreLearning product for a period of two years, ExploreLearning will provide written notice that the student data pertaining to their district will be destroyed, unless the district requests the records be kept. Upon destruction, ExploreLearning will provide written verification that the data has been destroyed.
6. ExploreLearning uses industry standard server and network hardware and software to ensure that data is protected from unauthorized access or disclosure.

Although we make concerted good faith efforts to maintain the security of personal information, and we work hard to ensure the integrity and security of our systems, no practices are 100% immune, and we can't guarantee the security of information. Outages, attacks, human error, system failure, unauthorized use or other factors may compromise the security of user information at any time. If we learn of a security breach or other unauthorized disclosure of your Personally Identifiable Information (PII), we will attempt to notify you so that you can take appropriate protective steps by posting a notice on our homepage

(www.explorelearning.com) or elsewhere in our Service and we will send email to you at the email address you have provided to us. Additionally, we will notify the primary administrative contact at your school or district by email and telephone and assist with their efforts to ensure your notification.

Any such notice will include:

- The date of the breach.
- The type of information that was subject to breach.
- General description of what occurred.
- Steps we are taking to address the breach.
- The contact person with our Company who you can contact regarding the breach.

If you are a parent, legal guardian or eligible student and an unauthorized disclosure of your student's PII records occurs, we will notify you by email at the email address we have on record for you or through notice to your school or district's primary administrative contact in the event that we do not have an email address on record for you.

When you use this site, you consent to our privacy practices and agree to accept the responsibilities **outlined in this statement.**

Contact

If you have any questions, concerns or inquiries about our Privacy Policy, or our use of your PII, or our privacy practices, please contact us at support@ExploreLearning.com, call at 888-399-1995, or mail to General Counsel 17855 Dallas Parkway, Suite 400 Dallas, TX 75287. You may also contact COPPAPrivacy@ikeepsafe.org.

ExploreLearning

Gizmos

This provides you with access to ExploreLearning's Data Management System. This system is an integral component of ExploreLearning's curriculum products and provides valuable reporting, instructional recommendations, and other resources used by teachers and other instructional leaders in conjunction with ExploreLearning's curriculum with the goal of improving student performance.

This statement describes the privacy and security practices ExploreLearning employs for this site. We have adopted these practices to protect you, the students, and the school district, and to enable each of us to comply with applicable legal requirements. Use of this site requires district acceptance of the practices outlined in this statement.

Two types of personally identifiable information are used on this site: **your personal data** and **student data**.

Your Personal Data

Collection

ExploreLearning collects information from you as you use this site. For example, you must enter certain personally identifiable information, including your name, e-mail address, and phone number. We use this information to verify your identity and prevent unauthorized access to your account and to contact you in connection with your use of this site.

In addition to the information you provide, ExploreLearning collects information about your use of this site through tracking, cookies, and log files, as described in our general Terms of Use statement.

Protection

Because you enter your personal data, you control its accuracy. If you discover that your personal data is inaccurate or if it changes or if you want to retain possession of it, you may make corrections by notifying us at support@ExploreLearning.com or 866-882-4141. We will not share your personal data collected through this site with third persons without your consent. However, your personal data will be available to authorized users from your school district who have permission from the school district to access it. We will not use your personal data collected through this site for any purpose other than providing you with access to this site and the associated services. We will use the same security to protect your personal data that we use to protect student data collected through this site.

Student Data

As you use this site, you will enter student data or interact with student data that has already been entered. Federal law (the Family Educational Rights and Privacy Act, "FERPA") allows a school district to release student records to an organization that is "conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests... [or] improving instruction."

However, FERPA requires limitations on disclosure of those records and implementation of appropriate security measures to protect those records. To help your school district comply with FERPA, ExploreLearning has adopted certain practices, and requires that educators using this site fulfill certain responsibilities to safeguard student data. Additionally, ExploreLearning operates in compliance with the Children's Online Privacy Protection Act ("COPPA") and obtains consent when necessary to collect information from children under 13 years of age.

The following statement explains our practices and your responsibilities regarding the student data you enter on this site.

Student Data Security and Confidentiality Statement

Purposes of Data Entry

You control what student data is entered on this site and you retain ownership of the student data at all times. Student data entered on this site should be limited to information that is relevant to the legitimate educational purpose of improving student performance. We will not ask you to enter, and you are instructed not to enter, data about students that is not relevant to this legitimate educational purpose.

Therefore, only a minimum amount of personally identifiable student data required for the setup of the system is requested. We require student first name, student last name, and student identification number. Additional data, not specific to the student, is also required to complete system setup, including the teacher first and last name, class name, grade level, and school name. Student demographic data, for the purposes of optional disaggregated reporting, is requested separately from the initial setup data and is obtained only with written permission from your district.

Use, Disclosure, and Storage

We will use the student data to provide the services to your school district. We will not keep the student data after you or the school district instructs us to delete it. You may not disclose or otherwise use the student data entered on this site for any unauthorized purposes.

We will only disclose student data to authorized employees or representatives of the school district, and will not knowingly disclose the student data to any third person without express written authorization. When, at the request of the district, we acquire assessment or other information, including personally identifiable student data, from a third party source we treat that information with the same confidentiality and security safeguards as though it were provided directly by the district. Additional agreements may be required by the third party to authorize transmission of data to ExploreLearning.

Your district may from time to time request that ExploreLearning provide student data to third parties of its choosing. We will do so with written authorization, which acknowledges that ExploreLearning is providing that data as your district's agent and that once the data is received by the third party, ExploreLearning no longer has any control over the use or disposition of the data.

We may also use aggregated data in our research, product development, and marketing. That aggregated, non-personally identifiable data (e.g., summary or statistical data) may be shared with third parties. However, we do not use personally identifiable student data to market any products or services directly to students or their parents.

In the event that ExploreLearning wishes, from time to time, to release aggregated data that identifies your school or school district by name, ExploreLearning will enter into a separate agreement with you to authorize release and publication.

ExploreLearning does not utilize third parties to provide products and does not share your student data with any third parties.

We may sell, transfer or otherwise share some or all of our assets, including your Personal Information, in connection with a merger, acquisition, reorganization or sale of assets or in the event of bankruptcy. Your consent to this Privacy Policy followed by your submission of Personal Information represents your explicit agreement to that transfer.

Data Quality

You are responsible for keeping the student data that you enter accurate, complete and up-to-date. If you recognize that student data is inaccurate, incomplete, or out-of-date, you are responsible for correcting it. If you experience problems making corrections to student data, please notify us at support@ExploreLearning.com and we will assist you with making corrections.

Security Safeguards

We are committed to protecting student data against unauthorized access, destruction, use, modification or disclosure. Protecting student data requires efforts from us and from you. We will implement reasonable and appropriate safeguards when collecting student data from you and when storing that student data in our database and you will observe our security safeguards and exercise reasonable caution when using this site.

Specific institutional and technological security safeguards include:

1. Only ExploreLearning employees who are authorized to handle student data are able to access the Data Management System.
2. Only school district employees and representatives that the district authorizes as school officials are permitted to access the system. It has a hierarchical permissions system. This means:

    a. A teacher will only be able to see data for his/her class.
    b. A Principal, Coach, or other authorized School User will be able to view all data at a given school.
    c. An authorized district-level employee, such as an Instructional Coordinator or Superintendent, will be able to see all data across the district.
3. Each authorized school official is given a Userid and Password valid only for the duration of the academic year, including a summer program if applicable. You must safeguard your Userid and Password, and not permit any unauthorized access to student data entered or kept in ExploreLearning's system.
4. Upon written request by the district, ExploreLearning will destroy any student data for districts who no longer participate in an ExploreLearning program. ExploreLearning will provide written verification that the data has been destroyed as requested.
5. If a district has not used any ExploreLearning product for a period of two years, ExploreLearning will provide written notice that the student data pertaining to their district will be destroyed, unless the district requests the records be kept. Upon destruction, ExploreLearning will provide written verification that the data has been destroyed.
6. ExploreLearning uses industry standard server and network hardware and software to ensure that data is protected from unauthorized access or disclosure.

Although we make concerted good faith efforts to maintain the security of personal information, and we work hard to ensure the integrity and security of our systems, no practices are 100% immune, and we can't guarantee the security of information. Outages, attacks, human error, system failure, unauthorized use or other factors may compromise the security of user information at any time. If we learn of a security breach or other unauthorized disclosure of your PII, we will attempt to notify you so that you can take appropriate protective steps by posting a notice on our homepage (www.explorelearning.com) or elsewhere in our Service and we will send email to you at the email address you have provided to us. Additionally, we will notify the primary administrative contact at your school or district by email and telephone and assist with their efforts to ensure your notification.

Any such notice will include:

- The date of the breach.
- The type of information that was subject to breach.
- General description of what occurred.
- Steps we are taking to address the breach.
- The contact person with our Company who you can contact regarding the breach.

If you are a parent, legal guardian or eligible student and an unauthorized disclosure of your student's PII records occurs, we will notify you by email at the email address we have on record for you or through notice to your school or district's primary administrative contact in the event that we do not have an email address on record for you..

When you use this site, you consent to our privacy practices and agree to accept the responsibilities outlined in this statement.

Contact

If you have any questions, concerns or inquiries about our Privacy Policy, or our use of your PII, or our privacy practices, please contact us at support@ExploreLearning.com or 866-882-4141, or mail to General Counsel 17855 Dallas Parkway, Suite 400 Dallas, TX 75287. You may also contact COPPAPrivacy@ikeepsafe.org.

Reflex

This provides you with access to ExploreLearning's Data Management System. This system is an integral component of ExploreLearning's curriculum products and provides valuable reporting, instructional recommendations, and other resources used by teachers and other instructional leaders in conjunction with ExploreLearning's curriculum with the goal of improving student performance.

This statement describes the privacy and security practices ExploreLearning employs for this site. We have adopted these practices to protect you, the students, and the school district, and to enable each of us to comply with applicable legal requirements. Use of this site requires district acceptance of the practices outlined in this statement.

Two types of personally identifiable information are used on this site: **your personal data** and **student data**.

Your Personal Data

Collection: ExploreLearning collects information from you as you use this site. For example, you must enter certain personally identifiable information, including your name, e-mail address, and phone number. We use this information to verify your identity and prevent unauthorized access to your account and to contact you in connection with your use of this site.

In addition to the information you provide, ExploreLearning collects information about your use of this site through tracking, cookies, cookies, and log files, as described in our general Terms of Use statement. Protection: Because you enter your personal data, you control its accuracy. If you discover that your personal data is inaccurate or if it changes or if you want to retain possession of it, you may make corrections by notifying us at support@ExploreLearning.com or 866-882-4141. We will not share your personal data collected through this site with third persons without your consent. However, your personal data will be available to authorized users from your school district who have permission from the school district to access it. We will not use your personal data collected through this site for any purpose other than providing you with access to this site and the associated services. We will use the same security to protect your personal data that we use to protect student data collected through this site

Student Data

As you use this site, you will enter student data or interact with student data that has already been entered. Federal law (the Family Educational Rights and Privacy Act, "FERPA") allows a school district to release student records to an organization that is "conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests... [or] improving instruction."

However, FERPA requires limitations on disclosure of those records and implementation of appropriate security measures to protect those records. To help your school district comply with FERPA, ExploreLearning has adopted certain practices, and requires that educators using this site fulfill certain responsibilities to safeguard student data. Additionally, ExploreLearning operates in compliance with the Children's Online Privacy Protection Act ("COPPA") and obtains consent when necessary to collect information from children under 13 years of age.

The following statement explains our practices and your responsibilities regarding the student data you enter on this site.

Student Data Security and Confidentiality Statement

Purposes of Data Entry: You control what student data is entered on this site and you retain ownership of the student data at all times. Student data entered on this site should be limited to information that is relevant to the legitimate educational purpose of improving student performance. We will not ask you to

enter, and you are instructed not to enter, data about students that is not relevant to this legitimate educational purpose.

Therefore, only a minimum amount of personally identifiable student data required for the setup of the system is requested. We require student first name, student last name, and student identification number. Additional data, not specific to the student, is also required to complete system setup, including the teacher first and last name, class name, grade level, and school name. Student demographic data, for the purposes of optional disaggregated reporting, is requested separately from the initial setup data.

Use, Disclosure, and Storage: We will use the student data to provide the services to your school district. We will not keep the student data after you or the school district instructs us to delete it. You may not disclose or otherwise use the student data entered on this site for any unauthorized purposes.
We will only disclose student data to authorized employees or representatives of the school district, and will not knowingly disclose the student data to any third person without express written authorization.
When, at the request of the district, we acquire assessment or other information, including personally identifiable student data, from a third party source we treat that information with the same confidentiality and security safeguards as though it were provided directly by the district. Additional agreements may be required by the third party to authorize transmission of data to ExploreLearning.

Your district may from time to time request that ExploreLearning provide student data to third parties of its choosing. We will do so with written authorization, which acknowledges that ExploreLearning is providing that data as your district's agent and that once the data is received by the third party, ExploreLearning no longer has any control over the use or disposition of the data.

We may also use aggregated data in our research, product development, and marketing. That aggregated, non-personally identifiable data (e.g., summary or statistical data) may be shared with third parties. However, we do not use personally identifiable student data to market any products or services directly to students or their parents.

In the event that ExploreLearning wishes, from time to time, to release aggregated data that identifies your school or school district by name, ExploreLearning will enter into a separate agreement with you to authorize release and publication.

ExploreLearning does not utilize third parties to provide products and does not share your student data with any third parties.

We may sell, transfer or otherwise share some or all of our assets, including your Personal Information, in connection with a merger, acquisition, reorganization or sale of assets or in the event of bankruptcy. Your consent to this Privacy Policy followed by your submission of Personal Information represents your explicit agreement to that transfer.

Data Quality: You are responsible for keeping the student data that you enter accurate, complete and up-to-date. If you recognize that student data is inaccurate, incomplete, or out-of-date, you are responsible for correcting it. If you experience problems making corrections to student data, please notify us at support@ExploreLearning.com and we will assist you with making corrections.
Security Safeguards: We are committed to protecting student data against unauthorized access, destruction, use, modification or disclosure. Protecting student data requires efforts from us and from you. We will implement reasonable and appropriate safeguards when collecting student data from you and when storing that student data in our database and you will observe our security safeguards and exercise reasonable caution when using this site.
Specific institutional and technological security safeguards include:

1. Only ExploreLearning employees who are authorized to handle student data are able to access the Data Management System.
2. Only school district employees and representatives that the district authorizes as school officials are permitted to access the system. It has a hierarchical permissions system. This means:
   A. A teacher will only be able to see data for his/her class.
   B. A Principal, Coach, or other authorized School User will be able to view all data at a given school.
   C. An authorized district-level employee, such as an Instructional Coordinator or Superintendent, will be able to see all data across the district.
3. Each authorized school official is given a Userid and Password valid only for the duration of the license period. You must safeguard your Userid and Password, and not permit any unauthorized access to student data entered or kept in ExploreLearning' system.
4. Upon written request by the district, ExploreLearning will destroy any student data for districts who no longer participate in an ExploreLearning program. ExploreLearning will provide written verification that the data has been destroyed as requested.
5. If a district has not used any ExploreLearning product for a period of two years, ExploreLearning will provide written notice that the student data pertaining to their district will be destroyed, unless the district requests the records be kept. Upon destruction, ExploreLearning will provide written verification that the data has been destroyed.
6. ExploreLearning uses industry standard server and network hardware and software to ensure that data is protected from unauthorized access or disclosure.

Although we make concerted good faith efforts to maintain the security of personal information, and we work hard to ensure the integrity and security of our systems, no practices are 100% immune, and we can't guarantee the security of information. Outages, attacks, human error, system failure, unauthorized use or other factors may compromise the security of user information at any time. If we learn of a security breach or other unauthorized disclosure of your PII, we will attempt to notify you so that you can take appropriate protective steps by posting a notice on our homepage (www.explorelearning.com) or elsewhere in our Service and we will send email to you at the email address you have provided to us. Additionally, we will notify the primary administrative contact at your school or district by email and telephone and assist with their efforts to ensure your notification.

Any such notice will include:

- The date of the breach.
- The type of information that was subject to breach.
- General description of what occurred
- Steps we are taking to address the breach.
- The contact person with our Company who you can contact regarding the breach.

If you are a parent, legal guardian or eligible student and an unauthorized disclosure of your student's PII records occurs, we will notify you by email at the email address we have on record for you or through notice to your school or district's primary administrative contact in the event that we do not have an email address on record for you.