

NEW YORK STATE MODEL DATA PRIVACY AGREEMENT
FOR EDUCATIONAL AGENCIES

Olean City School District

and

ExploreLearning, LLC

This Data Privacy Agreement ("DPA") is by and between the Olean City School District ("EA"), an Educational Agency, and ExploreLearning, LLC ("Contractor"), collectively, the "Parties". This DPA supplements Contractor's Quote, and each existing and subsequent agreement for Contractor's subscriptions and/or services, which are incorporated herein by reference.

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to

transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian or person in parental relation to the Student.
- 10. Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 13. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 14. Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 15. Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 16. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to upon completion ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34

CFR Part 98); the Individuals with Disabilities Education Act (“IDEA”) at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education’s Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law.

Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations, (hereafter, “Applicable Law”).

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement.

Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies that requirements under Applicable law and the EA’s policies reflecting such requirements. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor’s Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA’s Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA’s data security and privacy policy reflecting the requirements under Applicable Law.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. Such copies may be made available in a form that does not violate Contractor’s own information security policies, confidentiality obligations, and applicable laws. In addition, upon request by the EA, Contractor will provide results of available audits, vulnerability assessments or reviews of Contractor’s security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA’s policies reflecting such requirements applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by EA at EA’s expense. In the event of Breach that is attributable to Contractor or its Subcontractors, Contractor will provide summary results of available audits, the vulnerability assessments or reviews of Contractor’s security safeguards, measures and controls as it pertains to alignment

with the requirements of New York State laws and regulations, the EA's policies reflecting such requirements applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the summary of the audit report to the EA. In the event of Breach that is attributable to Contractor or its Subcontractors, Contractor may provide the EA with a summary of a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If Contractor determines at any point that a subcontractor has failed to materially comply with the requirements of this DPA and that a Breach has occurred, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is Breach by a subcontractor, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party without the prior written authorization of the EA unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. Data Return and Destruction of Data.

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract containing PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.
- (c) If requested, Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

9. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

10. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

11. Breach.

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

- (b) Notifications required under this paragraph must be provided to the EA at the following address:

Name: *Marc Friends*

Title: *Technology Coordinator/District Privacy Officer*

Address: *410 West Sullivan Street*

City, State, Zip: *Olean, NY 14760*

Email: *DPO@oleanschools.org*

12. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or

participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

13. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

14. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

3. Cyber Insurance.

If the Vendor will be communicating with the District electronically and/or collecting any sensitive staff or student data, the Vendor must have coverage applicable to first- and third-party claims including but not limited to data compromise expenses and liability, forensic review costs, legal review costs, data restoration and re-creation costs, public relations costs, extortion costs, network security liability, identity recovery costs, regulatory fines and penalties, and credit monitoring costs. Coverage limits shall be no less than:

Each Occurrence/Claim	\$1,000,000
Aggregate	\$1,000,000

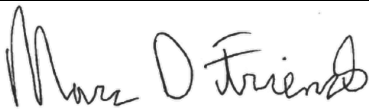

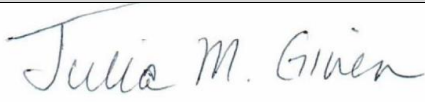
EDUCATIONAL AGENCY	CONTRACTOR
BY: <i>[Signature]</i> 	BY: 
Marc D Friends	<i>Julia M Given</i>
Technology Coordinator/District Privacy Officer	VP Finance
Date: 8-9-2022	Date: 8/9/22

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: <https://www.oleanschools.org/Page/8316>, by email to DPO@oleanschools.org. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	
[Printed Name]	Julia M Given
[Title]	VP Finance

Date:

8/9/22

EXHIBIT B

**BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -
SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE
INFORMATION**

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	ExploreLearning, LLC
Description of the purpose(s) for which Contractor will receive/access PII	Product update and enhancement notifications and in a customer service capacity when replying to support inquiries.
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date _____ Contract End Date _____
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input checked="" type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>Privacy: Please see attached Exhibit D</p> <p>Terms of Use: Please see attached Exhibit E</p>
Encryption	Data will be encrypted while in motion and at rest.

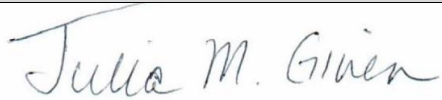
CONTRACTOR	
[Signature]	
[Printed Name]	Julia M Given
[Title]	VP Finance
Date:	8/9/22

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Privacy: Please see attached Exhibit D Terms of Use: Please see attached Exhibit E
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Cambium Learning employs application, database, and information controls to protect the system (potentially including the data, the database applications or stored functions, the application and database systems, the application and database servers and the associated network) against compromises of their confidentiality, integrity, and availability. This involves various types of controls that are technical, procedural/administrative and physical. These controls are meant to minimize: The risks of unauthorized or unintended activity or misuse by authorized users, system administrators, network/systems managers, or by unauthorized users (e.g. inappropriate access to sensitive data, metadata or functions within databases, or inappropriate changes to the application or database programs, structures or security configurations) Malware infections causing incidents such as unauthorized

		<p>access, leakage or disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized access to the database, attacks on other systems and the unanticipated failure of database services</p> <p>Overloads, performance constraints and capacity issues resulting in the inability of authorized users to use applications or databases as intended</p> <p>Physical damage to application or database servers</p> <p>Design flaws and programming bugs in databases and the associated programs and systems, creating various security vulnerabilities (e.g. unauthorized privilege escalation), data loss/corruption, performance degradation etc.</p> <p>Data corruption and/or loss caused by the entry of invalid data or commands, mistakes in database or system administration processes</p>
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	Security awareness training is required annually of all employees and contractors, covering FERPA, CCPA, social engineering, work-from-home security, and other topics
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	We conduct background checks for all new employees before they are hired and given access to our network. They are required to sign non-disclosure agreements and to read and acknowledge many of our critical policies. Access to systems is formally requested by supervisors and tracked in our IT help desk system. As well, The Company has a formal onboarding and off-boarding procedure where access to database assets is formally granted and revoked respectively; access is only granted to employees/contractors who need access to support the

		online products. The Company provides student data privacy training to all employees and contractors who access our network.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	The outline of our process is 1) verify the data breach, 2) contain and mitigate the data breach, 3) determine scope and composition of data breach, 4) analysis and communication planning, 5) notification, 6) post-notification and breach response review.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon written request by the district, ExploreLearning will destroy any student data for districts who no longer participate in an ExploreLearning program. 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.
7	Describe your secure destruction practices and how certification will be provided to the EA.	As database equipment is retired, it is provided to a computer recycling company, which destroys any persistent data. Our recycling company provides certificates of destruction. This data destruction is compliant with NIST 800- 88
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Privacy: Please see attached Exhibit D Terms of Use: Please see attached Exhibit E
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Privacy: Please see attached Exhibit D
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Our company has a clear mission with clear objective and clear organizational responsibilities. We have a part of our company dedicated and focused on cybersecurity and risk management.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Our legal department collaborates closely with other parts of the organization to ensure that all of the company's regulatory requirements are being met. We also have parts of the organization who focus on operational effectiveness. We also have a department who focus on the company's risks relating to cybersecurity and privacy.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	The company conducts a formal risk assessment annually and creates a risk treatment plan to address any risks which need to be mitigated.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	The company conducts a formal risk assessment annually and creates a risk treatment plan to address any risks which need to be mitigated.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the	Our key vendors are carefully chosen, and once chosen we purchase all of our assets from these main suppliers.

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	We operate on the principle of least privilege. We also have documented procedures on onboarding and off-boarding employees and contractors who have access to our network and systems. We also have a formal, documented process for granting people access to our various systems. We also hire 3rd party auditors to review and test our access controls annually.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	We require security awareness training annually for all employees and contractors who have access to our network.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	We operate with the least privilege principle. We also has system owners who are responsible for the CIA of their systems.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	We have several policies and procedures to manage the security and privacy of our systems. We also have a formal Information Security and Information Privacy Management System.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	We continuously monitor our network and application operations. We also keep all of our system patched and current.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	We use 3rd party monitoring services to ensure our systems are available and secure. We also run vulnerability scans throughout our network and on our online products to ensure all known vulnerabilities are addressed.
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	We monitor for denial of service and distributed denial of service attacks.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	We monitor for denial of service and distributed denial of service attacks. We also use email filtering services to help eliminate spam and phishing attacks.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	We use 3rd party services to monitor our public IP addresses and access to our online products from several locations throughout the US. We also log all authentication attempts.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed	We have policies and procedures to manage security incidents.

Function	Category	Contractor Response
	and maintained, to ensure response to detected cybersecurity incidents.	
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	We have policies and procedures to manage security incidents and breaches.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Our breach process calls for post mortems to improve our security posture.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Our incident response procedures address how to deal with a security event which can include blocking certain IP addresses, taking an endpoint or server off the network, etc.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	We do review our incidents and anomalies and strive to learn from them.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	We do have recovery procedures and technologies like backups to ensure we can successful recover from small and major incidents.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	We do review all required recoveries to determine if improvements need to be made.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Our incident management process and breach response process call for the close collaboration with all affected stakeholders and appropriate law enforcement agencies.

Exhibit D

Privacy Policy

This site 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.
 7. 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 (<https://gizmos.explorellearning.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.

Exhibit E

Terms and Conditions of Use

Please read these terms and conditions carefully before activating your ExploreLearning Gizmos account.

Gizmos are certified COPPA, FERPA, and CSPC compliant.

By creating an account or subscribing to ExploreLearning.com, you agree to the terms and conditions of use set forth below.

This Agreement is a legal document that governs the terms and conditions of your subscription to ExploreLearning.com. Please read this Agreement carefully. By activating your account, you acknowledge your agreement with these terms and conditions, as such terms and conditions may be amended from time to time. You are also agreeing to accept a non-exclusive, non-assignable right and license to use ExploreLearning Gizmos. ExploreLearning reserves the right to change these terms and conditions at any time.

ExploreLearning Gizmos are offered and sold on a subscription basis; however certain areas are available to visitors without cost on a trial or demonstration basis.

Registering and Using ExploreLearning

As part of the registration process, each User will select a password and user name ("User Name"). You agree to provide us with accurate, complete, and updated Account information. Failure to do so will constitute a breach of this Agreement, which may result in immediate termination of your rights to use the Account. You may not (a) select or use a User Name of another person with the intent to impersonate that person, (b) use a name subject to the rights of any other person without authorization, or (c) use a User Name that we, in our sole discretion, deem inappropriate or offensive. You are responsible for maintaining the confidentiality of your User Name and password, and you will be responsible for all uses of your User Name and password, whether or not authorized by you.

In order to use the Website, you need to obtain a pass code (consisting of a username and a password. Pass codes are issued only to individual subscribers and learning institutions or teachers (collectively, "Users") who have registered.

Pass codes that have been issued to learning institutions or teachers may not be shared. They may only be used by the administrators, teachers and students to whom they are assigned. Users remain at all times solely and fully responsible for the proper use of pass codes issued hereunder. Individual subscribers may share their access codes with their, spouse, children or grandchildren ("Immediate Family") only. Users remain at all times solely and fully responsible for the proper use of pass codes issued hereunder. Individual subscribers who intend to share their pass codes with Users of their Immediate Family under 13 years of age agree to supervise the minors' use of the Website.

Using Your Account

All Users are entirely liable for all activities conducted through that Account, and are responsible for ensuring that any other person who uses the Account is aware of, and complies with, the terms of this Agreement. Each person who uses the Account agrees to be bound by the terms of this Agreement, whether or not such person is a Member. You will notify us of any known or suspected unauthorized use(s) of your Account, or any known or suspected breach of security, including loss, theft, or unauthorized disclosure of your User Name and password. We will have no liability for any

circumstances arising from the unauthorized use of a User Name, Member's password or your Account. Any fraudulent, abusive, or otherwise illegal activity on your Account may be reported to appropriate law-enforcement agencies by us.

If you have reason to believe that your Account is no longer secure (for example, in the event of a loss, theft, or unauthorized disclosure or use of your User Name, password, or any credit, debit, or charge card number stored on the Service), you must promptly change your password and notify us of the problem by sending an email to support@ExploreLearning.com.

Browsers, Equipment and Accessibility

Users are solely responsible for obtaining and maintaining equipment and software, including without limitation operating system and browser software, that conforms to ExploreLearning's specifications in effect, as revised from time to time, in order to connect to, communicate with and use the ExploreLearning website.

ExploreLearning shall use commercially reasonable efforts to maintain the accessibility of the Website at all times, but may discontinue some or all of the Website features or services at any time, with or without notice, in order to perform hardware or software maintenance and/or upgrades or problem resolution. Additionally, to the extent that use of the Website is prevented, hindered, delayed or made impracticable by reason of force majeure (including any cause that cannot be overcome by reasonable diligence and without unreasonable expense) or due to ExploreLearning's compliance with its commercially reasonable standard operating procedures or with any laws, rules, policies, practices or regulations of any industry association or organization, or any jurisdiction or governmental authority, ExploreLearning and its affiliates will be excused from such delay or performance.

Communications Authorities

Use of the Website is subject to the requirements, rules, regulations, operations and procedures of any relevant public communications authorities and/or private communications carriers. ExploreLearning (and its affiliates) shall not be liable for any losses, costs, liabilities, damages, expenses and/or claims arising from or relating to the delay, alteration or interruption of telecommunications between Users and ExploreLearning caused by the failure for any reason of any communications facilities which User or ExploreLearning (or any of affiliate) has contracted from any public communications authority or private communications carrier.

Billing Policies

1. All subscriptions must be pre-paid annually.
2. Payment Options: You must pay in US Dollars via Purchase Order, Credit Card (Visa or MasterCard), check or money order, or wire transfer.
 - Purchase Orders (US Residents Only): Mail (payable to ExploreLearning) to ExploreLearning, 110 Avon Street, Charlottesville, VA 22902 or FAX to (877) 829-3039.
 - Credit Card Billing: ExploreLearning will bill your designated credit card (Visa or MasterCard only) and is subject to any restrictions imposed by your credit card issuer. If payment cannot be charged to your credit card or your charge is returned to ExploreLearning for any reason, including charge back, ExploreLearning reserves the right to either suspend or terminate your access and account, thereby terminating this Agreement and all obligations of ExploreLearning hereunder, and thereafter to collect any amount due.
 - Checks or Money Orders: Mail (payable to ExploreLearning) to ExploreLearning, 110 Avon Street, Charlottesville, VA 22902.
 - Wire Transfers: Call (866) 882-4141 option 2 or e-mail support@ExploreLearning.com for more information

3. **Revision of Subscription Fees.** ExploreLearning reserves the right to change the amount of, or basis for determining, any fees or charges for the ExploreLearning service, and to institute new fees or charges effective upon prior notice, by posting such changes on the ExploreLearning site, and by sending e-mails to Users.

4. **Account Termination.** Purchasers may terminate accounts at any time by sending a signed request to ExploreLearning via e-mail sales@ExploreLearning.com , fax to (877) 829-3039 or mail to ExploreLearning Customer Service, 110 Avon Street, Charlottesville, VA 22902.

5. **Refund Policy.** We take great pride in supplying a quality product at a reasonable price. In general, it is our policy to provide a refund for anyone who has been unable to use the site. A refund must be requested in writing within 30 days of purchase of your account and the account cannot have been accessed numerous times. Email a refund request to sales@ExploreLearning.com or fax a request to (877) 829-3039. Please include the username, full name of subscriber, product, and reason you are requesting a refund. We will not be able to refund a license after 30 days, or for an account with heavy usage, except for problems accessing the service. Refunds will be issued according to the original payment method.

Billing Security

All communication between our servers, the acquiring bank, and the issuing bank are encrypted to assure server authenticity and invulnerability to man-in-the-middle attacks.

Administering the Service

ExploreLearning may change, modify, suspend, or discontinue any aspect of the Website at any time, including, without limitation, access policies, the availability of any Website feature, hours of availability, content, data, or software or equipment needed to access the Website. We may also impose limits on certain features or restrict your access to parts or all of the Website without notice or liability. We reserve the right to change prospectively the amount of, or basis for determining, any fees or charges for the Website, and to institute new fees or charges for access to portions of the Website effective upon prior notice to Users by posting such changes on its web site or by sending e-mails to Users. You hereby agree to pay all charges to your account, including applicable taxes, in accordance with billing terms in effect at the time the fee or charge becomes payable.

We may, from time to time, have special events, software or content available on the Service, which will be subject to additional terms and conditions that will be made available for your review. You agree that if you or any User uses or accesses such special events, software or other content, such additional terms and conditions will be binding.

We reserve the right, at our sole discretion, to change, modify, add, supplement or delete any of the terms and conditions of this Agreement at any time. We will post notification of any such changes on the Service, or give notice of them to you via e-mail, postal mail or by pop-up screen, at our sole discretion. If any future changes to this Agreement are unacceptable to you or cause you to no longer be in compliance with this Agreement, you may terminate your Account. The continued use of the Service by you following your receiving a notice of changes to this Agreement will mean you accept any and all such changes.

Posting Material by Users

ExploreLearning may permit its Users to post materials on the Website. Users shall not upload to, distribute through or otherwise publish, via e-mail, message boards or otherwise, any content which is libelous, defamatory, obscene, threatening, invasive of privacy or publicity rights, abusive, illegal or otherwise objectionable, that would constitute a criminal offense, violate the rights of any third party, or that would give rise to liability or violate any law.

ExploreLearning reserves the right to suspend or terminate any screen name it reasonably believes is being used by an adult, is being used for commercial purposes, or is otherwise in violation of this Agreement.

By uploading materials to any message boards, lesson plans or other posting areas, or otherwise submitting any materials to us, you automatically grant (or warrant that the owner of such rights has expressly granted) us a perpetual, royalty-free, irrevocable, non-exclusive right and license to use, reproduce, modify, adapt, publish, translate or create derivative works from and distribute such materials or incorporate such materials into any form, medium, or technology now known or later developed throughout the World. In addition, you warrant that all so-called "moral rights" in those materials have been waived.

Use of Materials & Restrictions

Permitted Use: You have our permission to print a reasonable number of copies of ExploreLearning content displayed on the Website for noncommercial personal or classroom use, provided that any copies you print continue to show all notices concerning copyright, trademark and other proprietary rights that appear in the material you reproduce.

Prohibited Uses: Except as expressly permitted by copyright law and except as permitted in the preceding paragraph, you must obtain written permission from ExploreLearning, or the third-party owner of material appearing on the Website, for any other copying, redistributing or publishing of any ExploreLearning or "Third Party Content." The downloading to a server or personal computer of ExploreLearning or Third Party Content displayed on the Website and the downloading of any code from the Website is strictly prohibited. You may not modify, publish, transmit, participate in the transfer or sale of, reproduce, create derivative works from, distribute, perform, display or in any way exploit, any of the ExploreLearning or Third Party Content, in whole or in part, for commercial purposes without the express permission of ExploreLearning.

Linking to and framing the Website: You may create and publish links to the ExploreLearning.com homepage at <https://gizmos.explorelearning.com>. Creating and publishing links to any other pages within the Website (except bookmarking such pages for your personal noncommercial use) is not permitted. Framing the Website is strictly prohibited.

Additional Restrictions: You may not: (a) access the Website by any means other than means supporting secure and encrypted communications; (b) copy, reverse engineer, disassemble, decompile, translate, or modify any Website application or service; (c) sublicense, rent, lease, or permit any third party, to access any Website application or service through the use of User's password, except as permitted hereunder; (d) publish the results of benchmark tests of any Website application or service, or use any Website application in any manner which is competitive with services provided by ExploreLearning; and (e) knowingly use or permit any others to use any facilities or services of ExploreLearning or its Licensors in connection with any effort that the User knows seeks to breach the security or confidentiality of any other digital or on-line environment.

Users understand that except for ExploreLearning Content, ExploreLearning does not control, provide, operate, and is not responsible for, any content, goods or services available on the Internet other than the ExploreLearning Content on the Website. Internet content made accessible on the Internet by independent third parties is not part of, and is not controlled by, ExploreLearning. ExploreLearning neither endorses nor is responsible for the accuracy or reliability of such Internet content, goods or services.

Users should be aware that the Internet contains content, goods and services that you may find obscene, improper, hurtful or otherwise offensive and that may not be suitable for certain users of the Website. Because of the nature of the Internet, we cannot control where children may go while using the Website. Parents, guardians or teachers should supervise children when using the Website and the Internet at all times.

Any unauthorized use may subject you to civil liability and criminal prosecution under applicable laws.

In the event you download software from ExploreLearning, the software, including any files, images incorporated in or generated by the software and data accompanying the software (collectively, the "Software"), are licensed to you by ExploreLearning. ExploreLearning, or our contract partners, does not transfer title to the Software to you. ExploreLearning, or our contract partners, retains full and complete title to the Software and all intellectual property rights therein. You may not redistribute, sell, decompile, reverse-engineer or disassemble the Software.

Privacy

ExploreLearning is committed to protecting the privacy of website visitors and does not share personally identifiable information with third parties without your consent. Please consult our Privacy Policy for more information on our information collection, use and disclosure practices. You acknowledge that, although ExploreLearning agrees to use its best efforts to comply with and to ensure that its users, content providers, distributors and licensees comply with our Privacy Policy, ExploreLearning cannot be held responsible for the actions of third parties who violate our Privacy Policy.

Submissions

If you send us creative suggestions, ideas, notes, stories, messages, narratives, drawings, concepts, or other information or content ("Submissions"), the Submissions will be deemed, and shall remain, the sole and exclusive property of ExploreLearning, and ExploreLearning will be entitled to the unrestricted use of the Submissions for any purpose whatsoever, without compensation to you. None of the Submissions shall be subject to any obligation of confidence on the part of ExploreLearning, and ExploreLearning shall not be liable for any use or disclosure of any Submissions. Without limiting the generality of the foregoing, ExploreLearning shall exclusively own all now known or hereafter existing rights to the Submissions of every kind and nature throughout the World, and shall be entitled to unrestricted use of the Submissions for any purpose whatsoever, commercial or otherwise.

DISCLAIMERS

DISCLAIMER OF WARRANTIES

YOU EXPRESSLY UNDERSTAND AND AGREE THAT:

YOUR USE OF THE SERVICE IS AT YOUR SOLE RISK. THE SERVICE IS PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. EXPLORELEARNING EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

EXPLORELEARNING MAKES NO WARRANTY THAT (I) THE SERVICE WILL MEET YOUR REQUIREMENTS, (II) THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE, (III) THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SERVICE WILL BE ACCURATE OR RELIABLE, (IV) THE QUALITY OF ANY PRODUCTS, SERVICES, INFORMATION, OR OTHER MATERIAL PURCHASED OR OBTAINED BY YOU THROUGH THE SERVICE WILL MEET YOUR EXPECTATIONS, (V) ANY ERRORS IN THE SOFTWARE WILL BE CORRECTED, (VI) OR THAT THIS WEBSITE, ITS CONTENT, AND THE SERVERS ON WHICH THE WEBSITE AND CONTENT ARE AVAILABLE ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS.

ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICE IS DONE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL.

NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM EXPLORELEARNING OR THROUGH, OR FROM, THE SERVICE SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED IN THE TOS.

INFORMATION CREATED BY THIRD PARTIES THAT YOU MAY ACCESS ON THE WEBSITE OR THROUGH LINKS IS NOT ADOPTED OR ENDORSED BY EXPLORELEARNING AND REMAINS THE RESPONSIBILITY OF SUCH THIRD PARTIES.

LIMITATION OF LIABILITY

YOU EXPRESSLY UNDERSTAND AND AGREE THAT EXPLORELEARNING SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, DATA OR OTHER INTANGIBLE LOSSES (EVEN IF EXPLORELEARNING HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES), RESULTING FROM: (I) THE USE OR THE INABILITY TO USE THE SERVICE; (II) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS AND SERVICES RESULTING FROM ANY GOODS, DATA, INFORMATION OR SERVICES PURCHASED OR OBTAINED OR MESSAGES RECEIVED OR TRANSACTIONS ENTERED INTO THROUGH OR FROM THE SERVICE; (III) UNAUTHORIZED ACCESS TO OR ALTERATION OF YOUR TRANSMISSIONS OR DATA; (IV) STATEMENTS OR CONDUCT OF ANY THIRD PARTY ON THE SERVICE; OR (V) ANY OTHER MATTER RELATING TO THE SERVICE. IN NO EVENT SHALL EXPLORELEARNING'S TOTAL LIABILITY TO YOU FOR ALL DAMAGES, LOSSES, AND CAUSES OF ACTION, WHETHER IN CONTRACT, NEGLIGENCE, TORT OR OTHERWISE EXCEED THE AMOUNT PAID BY YOU, IF ANY, FOR ACCESSING EXPLORELEARNING.

Links to Third Party Sites

ExploreLearning may contain links to other websites operated by parties that are not affiliated with it. These links will let you leave ExploreLearning to visit websites not under ExploreLearning's control. ExploreLearning is not responsible for the contents of any linked website or any link contained in a linked website. We provide these links to you only as a convenience, and the inclusion of any link does not imply endorsement of the linked site by ExploreLearning.

Jurisdictional Issues

ExploreLearning makes no representation that materials on ExploreLearning are appropriate or available for use in all locations. Those who choose to access ExploreLearning do so on their own initiative and are responsible for compliance with local laws, if and to the extent local laws are applicable. Software from ExploreLearning is further subject to United States export controls. No software from ExploreLearning may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. By downloading or using the Software, you represent and warrant that you are not located in, under the control of, or a national or resident of any such country or on any such list.

Trademark and Copyright Notices

Copyright© 2018 ExploreLearning. All rights reserved. ExploreLearning, ExploreLearning Gizmos, Gizmo and Gizmos and/or all other logos, names and services on the ExploreLearning.com website are trademarks of ExploreLearning. Outside of the ReflexMath.com website, the words "ExploreLearning," "ExploreLearning Gizmos," and "EL Gizmos" are trademarks of ExploreLearning. Other trademarks and names are the property of their respective owners.

Permission to reprint screen shots from ExploreLearning.com for commercial use may be requested at support@ExploreLearning.com .

Remedies for Breach

In the event that ExploreLearning determines, in its sole discretion, that a User has breached any portion of these terms and conditions, or has otherwise demonstrated inappropriate conduct, we reserve the right to (i) warn the User via e-mail that she or he has violated this Agreement; (ii) delete any content provided by the User (or anyone accessing User's account); (iii) discontinue the User's account and/or any other ExploreLearning service; (iv) notify and/or send content to and/or fully cooperate with the proper law enforcement authorities for further action; and/or (vi) take any other action that ExploreLearning deems appropriate.

Miscellaneous

In the event any provision of this Agreement conflicts with the law or if any such provisions are held invalid by a court with jurisdiction over the parties to this Agreement, such provision will be deemed to be restated to reflect as nearly as possible the original intentions of the parties in accordance with applicable law, and the remainder of this Agreement will remain in full force and effect.

The laws of the State of Texas will govern this Agreement. The laws of the State of Texas will govern any dispute arising from the terms of this agreement or breach of this agreement and you agree to personal jurisdiction by the state and federal courts sitting in Dallas, Texas. The parties hereby expressly waive trial by jury in any action, proceeding or counterclaim brought by either of the parties against the other on any matters whatsoever arising out of, or in any way connected with, these Terms and Conditions and agree to submit to binding arbitration. ExploreLearning makes no representation that materials on ExploreLearning are appropriate or available for use in all locations. Those who choose to access ExploreLearning do so on their own initiative and are responsible for compliance with local laws, if and to the extent local laws are applicable. Materials from ExploreLearning are further subject to United States export controls. No materials from ExploreLearning may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Commerce Department's Table of Deny Orders. By downloading or using the materials, you represent and warrant that you are not located in, under the control of, or a national or resident of any such country or on any such list.

The failure of either party to insist upon or enforce strict performance by the other party of any provision of this Agreement or to exercise any right under this Agreement will not be construed as a waiver or relinquishment to any extent of such party's right to assert or rely upon any such provision or right in that or any other instance, rather, the same will be and remain in full force and effect.

ExploreLearning may assign its rights and obligations under this Agreement and upon such assignment ExploreLearning may be relieved of any further obligation hereunder. You represent to ExploreLearning that you have the authority to subscribe to and/or use ExploreLearning according to the terms and conditions of this Agreement. The section titles in this Agreement are for convenience only and have no legal or contractual effect.

Acceptance

By using and/or subscribing to the Service, you hereby acknowledge that you have read and understand the foregoing Agreement, as may be amended or modified from time to time according to its terms, and agree to be bound by all of

the terms and conditions hereof. You further specifically permit ExploreLearning to use the email entered during the registration process to deliver support, sales, and product information related to your Free Trial or paid subscription.

Questions

If you have any questions about this Agreement, please email us at: support@ExploreLearning.com .