

EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

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

1. Purpose

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

2. Definitions

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

In addition, as used in this Exhibit:

- (a) “Student Data” means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (b) “Teacher or Principal Data” means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.
- (c) “Protected Data” means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor’s Product.

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

3. **Confidentiality of Protected Data**

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

4. **Data Security and Privacy Plan**

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

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

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

Attached on next 5 pages



Privacy Statement

This Privacy Statement is incorporated in, and subject to, the Terms of Use and Service for Imagination Station, Inc. ("**Istation**"). Please refer to those terms for definitions of words with initial capitals letters that are not otherwise defined in this Privacy Statement. Istation encourages you to read this Privacy Statement carefully.

For purposes of this Privacy Statement, references to "**You**" or "**Your**" mean (i) you in your individual capacity, (ii) your company, which may be a school or school district, and (iii) students, employees, representatives and agents of Your school or school district that are registered with Istation and that have a valid security identification and password to access and use the Resources (collectively the "**Authorized Users**").

As noted in the Terms of Use, Istation provides its customers with a range of educational resources, including, but not limited to, (i) Istation's interactive educational-based applications (collectively the "**Licensed Applications**"), (ii) Istation's Internet Web site (the "**Web Site**"), currently located at www.istation.com, (iii) account information regarding the Licensed Applications and the Web Site, (iv) materials and documentation (including, but not limited to, preprinted forms, form letters, resource materials, lesson plans, books, images of Istation characters, and so-called "Black Line Masters" coloring-book style pictures) available from the Web Site (collectively the "**Downloadable Materials**"), and (v) news and information about Istation, the Licensed Applications, and the Web Site. Any and all of the foregoing resources (including, but not limited to, the Licensed Applications, the Web Site, and the Downloadable Materials), together with any other resources made available by Istation, are collectively referred to as the "**Resources**".

What Personally Identifiable Information Is Collected by Istation?

"**Personally Identifiable Information**" generally refers to any data that could potentially identify a specific individual. While You have access to the Resources, Istation may collect the following Personally Identifiable Information about You:

- Your first and last name
- **Teachers and administrators only** – Your contact information, such as email addresses, mailing addresses, and phone numbers
- Your school and school district
- Any identification numbers issued by Your school and/or Your school district to You, including teacher numbers, administrator numbers, and student numbers;
- Security information, such as usernames, passwords, and password hints;
- Browser information, such as browser version, IP address, and the presence of various plug-ins and tools;



- **Students only** – “Demographic Data,” such as gender, race, special-education status, socio-economic status, and English language learner status, but only to the extent provided by Your school or Your school district;
- Resource-related responses submitted by You, including, but not limited to responses to interactive activities and assessments;
- Resource use behavior, such as pages visited, downloads, or searches requested; and
- Resource use results, but only to the extent that such results identify one or more (i) students, (ii) teachers, (iii) classrooms within an identified school, (iii) grades within an identified school or school district or (iv) schools (collectively “**Identifiable Use Results**”). Identifiable Use Results do not include Resource use results for school districts or for geographic regions that do not identify a specific school (such as Resource use results reported (i) on a county-wide basis, (ii) within a defined territory [whether officially or unofficially defined], such as North Texas, or (iii) within a metropolitan area, such as Dallas-Fort Worth).

Personally Identifiable Information does not include “De-identified Information,” which is any data or information that cannot be traced back to an individual (except for Identifiable Use Results, as defined above). For example, a table listing the number of students in each grade at a specific school using a particular Resource would not be Personally Identifiable Information.

How Is Personally Identifiable Information Used and/or Disclosed?

Istation does not sell Personally Identifiable Information to any affiliated entity of Istation or any third-party, nor does it use such information for any sort of behavioral advertising. However, Istation may use and disclose Personally Identifiable Information for a range of educational, compliance and quality assurance purposes.

Istation may use Personally Identifiable Information for the following purposes:

- To provide status reporting notices to teachers and administrators about the Resources (e.g. – an email prompting a teacher to log in to see his or her students’ latest assessment results);
- To internally analyze data regarding the use of the Resources;
- To track students’ usage of the Resources over time, including performance metrics collected over multiple school years;
- To send You (**teachers and administrators only**) updates, promotional/advertising materials, and newsletters related to the Resources and Istation’s products and services or to otherwise market specific Istation services or offers to You. If You want to stop receiving promotional/advertising/ marketing materials from Istation, You will have the option to unsubscribe;
- To respond to Your questions or comments; and
- To customize content within the Resources, to improve the Resources’ content and functionality and to develop new products and updates.



Istation may disclose Personally Identifiable Information to the following individuals or entities under the following circumstances:

- To Istation's employees who need to access the Personally Identifiable Information to perform their jobs;
- To third parties, including contractors, vendors, and service providers, that assist with the production, implementation or servicing of the Resources, but only after receiving satisfactory assurances from each third-party that its data privacy and security protections are at least as stringent as those of Istation;
- To Authorized Users as determined by each school or school district at issue. Generally, but subject to determination by the school at issue or the school district at issue,
 1. a teacher may only see the Personally Identifiable Information of the students in the teacher's classroom,
 2. a principal may only see the Personally Identifiable Information of those students and teachers in the principal's school, and
 3. a school district-level administrator may only see the Personally Identifiable Information of those students and teachers in the administrator's school district;
- To third parties, and solely for educational purposes, when Istation has the consent of the school or school district at issue, including Identifiable Use Results that identify specific individual students if Istation has received a written acknowledgement from the school or school district that it has obtained the student's consent to such disclosure;
- When Istation believes that sharing Personally Identifiable Information is reasonably necessary in order to (i) protect or defend the legal rights, interests, property, safety, or security of Istation, its employees or contractors, or the public, (ii) protect or defend against, or otherwise address, fraud, security, or technical issues, (iii) comply with, or respond to a law, regulation, legal request, legal process, legal requirement, judicial proceeding, or court order, or (iv) investigate a possible crime, such as fraud or identity theft;
- In connection with an actual or potential sale, purchase, acquisition, merger, reorganization, bankruptcy, liquidation, dissolution, or similar transaction or proceeding of or involving Istation, but only to the extent that the purchasing, acquiring or successor entity agrees to implement data privacy and security protections with respect to Personally Identifiable Information that are at least as stringent as those of Istation.

Istation is permitted to use and/or disclose Personally Identifiable Information about You when Istation has Your consent. Istation does not need Your consent to use De-identified Information.



Can I Access or Change My Personally Identifiable Information?

Each school and/or school district is permitted via functionality made available by the Resources to determine what Personally Identifiable Information (if any) is accessible by Authorized Users and to which Authorized Users in particular. In certain circumstances, a school and/or school district may be entitled to permit one or more Authorized Users to change Personally Identifiable Information. Any requests by Students or parents to access and/or change Personally Identifiable Information must be made to the school and/or school district in the first instance, and these entities will maintain a record of all such access and amendment requests and of any actual changes made. To the extent that a student and/or parent makes a direct request to Istation to access and/or amend Personally Identifiable Information, Istation will forward that request to the school and/or school district for response.

Data Retention

Unless required by law to maintain certain information for a longer period of time, Istation retains Personally Identifiable Information only for as long as a student's school and/or school district maintains a subscription with Istation to one or more of the Resources. Once a subscription to a particular Resource is cancelled or otherwise terminated, Istation will typically retain any Personally Identifiable Information related to that Resource for sixty days after cancellation/termination to allow for temporary lapses in subscription services, at which point that information is destroyed. Personally Identifiable Information may also be destroyed at any time at the request of the school and/or school district.

Website and Resource Security

Istation recognizes its responsibility to protect the Personally Identifiable Information that You entrust to it. Istation uses a variety of secure techniques to protect Your information, including secure servers, firewalls, access limitations on Istation's servers and password protections that guard against unauthorized access. Additionally, the information that You send Istation via the Website, including student usage information and passwords, may be encrypted, a process used to scramble information and make it extremely difficult to read if wrongly intercepted. Istation utilizes industry standard Secure Sockets Layer (SSL) technology to allow for the encryption of Personally Identifiable Information. All Personally Identifiable Information sent to Istation is encrypted during transmission, such as during login. Once the data reaches Istation's server, Personally Identifiable Information is stored on a secure database, and access to this information is password protected.



Use of “Cookies”

“Cookies” are small pieces of information that some websites store on Your computer’s hard drive when You visit them. This element of data is a piece of text, not a program, that contains information identifying a user. When a user revisits a Website, his or her computer automatically “serves up” the cookie, eliminating the need for the customer to reenter the information. Like many other websites, Istation uses cookies for this purpose. Your user “domain” (that is, Your school name) is the only data stored on Your hard drive by Istation.

Most web browsers automatically accept cookies but allow You to modify security settings so You can approve or reject cookies on a case-by-case basis. At a minimum, Your web browser must allow temporary cookies that are not stored on Your hard disk to log into the Website. Please refer to the “Help” file of Your Internet Browser either to learn how to receive a warning before a cookie is stored.

Third Party Sites

The Website may contain links to or reference third party websites and resources (collectively “Third Party Sites”). These Third Party Sites are not controlled by Istation and, therefore, are not subject to this Privacy Statement. You should check the privacy policies of these individual Third Party Sites to see how Your personally identifiable information will be utilized by them before providing any personally identifiable information. Please be aware that these Third Party Sites may collect personally identifiable information about You and may also send you “cookies.” Istation is not responsible for the content or practices of any linked Third Party Sites, and Istation provides these links solely for the convenience and information of Istation’s visitors.

Can Istation change this Privacy Statement?

Istation may change this Privacy Statement at any time without advance notice. However, if the Privacy Statement changes, Istation will post an updated version on the Website, and the revision date will be posted at the bottom of the page. If this occurs, You will be required to re-acknowledge review of the revised Privacy Statement before you can continue using the Resources.

Who can I contact if I have questions about this Privacy Statement?

If You have any questions about this Privacy Statement or any privacy questions or concerns, You may contact Istation using the information below:

Email address: info@Istation.com
Street/Postal address:
 8150 North Central Expressway, Suite 2000
 Dallas, Texas 75026

Phone: (214) 237-9300
Fax: (972) 643-3441
Effective Date: February 23, 2018

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

5. **Additional Statutory and Regulatory Obligations**

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

- (a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).
- (b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.
- (c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.
- (d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

- (i) the parent or eligible student has provided prior written consent; or
 - (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.
- (e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody.
- (f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.
- (h) Promptly reimburse Erie 1 BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to Vendor or its subcontractors or assignees.

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

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

("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

- (e) Vendor will consult directly with Michelle Okal-Frink or her designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

EXHIBIT D (CONTINUED)**PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

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

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at <http://www.nysed.gov/data-privacy-security/student-data-inventory>, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>.

BY THE VENDOR:

Signature

Robert Rubin
Printed Name

Chief Information Officer
Title

09-08-2023
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND ISTATION

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

Istation Reading
Istation Lectura
Istation Math
ISIP Reading assessment
ISIP Lectura assessment
ISIP Math assessment
The Story of America US History curriculum

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

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

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

N/A – No subcontractors will be used]

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2023 and expires on June 30, 2026.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data. If requested by

Erie 1 BOCES and/or any Participating Educational Agency, Vendor will assist a Participating Educational Agency in exporting all Protected Data previously received back to the Participating Educational Agency for its own use, prior to deletion, in such formats as may be requested by the Participating Educational Agency.

- In the event the Master Agreement is assigned to a successor Vendor (to the extent authorized by the Master Agreement), the Vendor will cooperate with Erie 1 BOCES as necessary to transition Protected Data to the successor Vendor prior to deletion.
- Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide Erie 1 BOCES with a certification from an appropriate officer that these requirements have been satisfied in full.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Vendor, by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Vendor by following the appeal process in their employing school district's applicable APPR Plan.

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

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