

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: [See attached Data Security and Privacy Plan]
- (c) Vendor will comply with all obligations set forth in Erie 1 BOCES' "Supplemental Information about the MLSA" below.

- (d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Vendor has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Vendor will require that all of its employees (or officers or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.
- (e) Vendor [*check one*] _____ will X will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontractors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.
- (f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.
- (g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

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

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

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

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

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

incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

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

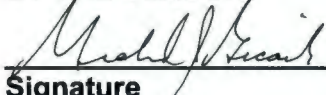
EXHIBIT D (CONTINUED)

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

Michael Gecawich
Printed Name

President & CEO
Title

April 13, 2022
Date

EXHIBIT D (CONTINUED)**SUPPLEMENTAL INFORMATION****ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND B.E. PUBLISHING**

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

eReadiness.com / The Digital Platform for College and Career Readiness

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: [No subcontractors are utilized.]

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on April 13, 2022 and expires on June 30, 2025.
- 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.

B.E. Publishing Data Security & Privacy Plan Overview

1) Compliance with New York State Education Law 2-D.

In the development, deployment, and management of our eReadiness.com platform, B.E. Publishing adheres to the data security and privacy requirements of all applicable federal and state laws, including those of the New York State Education Law Section 2-d.

2) Process by which student data and/or principal or teacher data is stored, secured, and encrypted.

Our data security safeguards align with the NIST Cybersecurity Framework and adhere to industry standards and best practices including but not limited to encryption, firewalls, and password protection when protected data is stored or transferred. Data we receive is stored on systems maintained under our direct control in a secure data center facility located within the United States.

Our data security safeguards utilize industry-recognized technical standards of software development and deployment, the successful implementation of which is reviewed, tested, and maintained by our standard operational management procedures (including limiting who has secured access to data and the daily vetting of system health), all of which is subject to administrative oversight, review, and confirmation (which assures that the technology and its development and deployment adhere to all contractual expectations vis-à-vis data security).

3) Process by which employees (and sub-contractors if used) receive training on the laws governing data prior to receiving access to the data.

Employees who will have access to student data or teacher or principal data receive training on the federal and state laws governing confidentiality of such data. Such training is provided as follows:

August – New school-year contract requirements are reviewed; data privacy expectations/requirements are reviewed and confirmed, requiring all staff with necessary access to secure data adheres to customer contract stipulations and other data protection regulations, e.g., FERPA, CORPA, CIPA.

January – New operational-year milestones/schedules are reviewed; customer data privacy expectations/requirements are reviewed and confirmed as above.

B.E. Publishing does not engage subcontractors to manage, process, or otherwise access any student data and/or principal or teacher data.

3) Process by which data security/privacy breaches are identified and managed, including remediation and notification.

Our standard operational procedures provision for daily monitoring of (product) system health, which includes a review of how and which database records are being accessed. This standard ensures that we become aware of any system anomaly which could signal a data breach.

In the event of a data breach, which means an unauthorized access, disclosure, alteration, or use of user or account data (or circumstances that could have resulted in such unauthorized access, disclosure, alteration, or use) we promptly institute the following:

- (1) notify the school/district by telephone and email as soon as practicable, but no later than twenty-four hours after we become aware of the data breach;
- (2) provide the school/district with the name and contact information for a B.E. Publishing employee who shall serve as our primary security contact;
- (3) assist the school/district with any investigation, including interviews with our employees and review of all relevant records; and
- (4) assist the school/district with any notification the school/district deems necessary related to the security breach;
- (5) immediately engage and implement any necessary administrative, technical, and physical measures to protect systems and data.

eReadiness.com Privacy Policy

January 10, 2022

eReadiness.com (a product of B.E. Publishing, Inc.) keeps all user and account information collected strictly private and confidential. All information we collect (as described herein) is used solely for educational purposes. We do not share, sell, or otherwise give away private information to anyone. At most, some non-personal information such as IP address and web browser version are made available to third-party services that allow us to improve and administer the site.

It is the policy of B.E. Publishing to adhere to, and cooperate with school districts in meeting all applicable privacy and security standards for the collection, storing, securing, and use of personal user information as set forth in state and federal regulations, such as the Family Educational Rights and Privacy Act ("FERPA") and Children's Online Privacy Protection Act ("COPPA").

B.E. Publishing, Inc. has created this privacy statement to demonstrate our firm commitment to privacy. This privacy policy applies to information, including personal information, that eReadiness.com collects when you use the eReadiness.com website.

eReadiness.com offers both a free trial version and a premium, licensed version. The personal information we collect is dependent upon the version utilized.

Access to Online Resources

eReadiness.com provides online access to a title's student and instructor resources (such as PDFs, digital media, and app-specific source files) and its e-texts. When a school or school district purchases a license for one or more title, we provide the designated school or district administrator with the title access code(s) for distribution to teachers, enabling them to access a title's instructor-only resources, including the title's e-text.

When an access code is first redeemed on eReadiness.com, the teacher creates a user profile consisting of a username or email address, password, first name, last name, and state or province.

Students do not receive access codes. Students have open access to the student resources of every title. Therefore, eReadiness.com does not directly collect any student data since students do not create a user profile to use eReadiness.com.

Information We Collect

We collect information from you directly when you create an account. eReadiness.com may send one or more cookies to your browser to help customize your experience on our site, such as logging into your account, viewing course preferences and progress.

You may establish an account with eReadiness.com by providing us with a username or email address, password, first name, last name, and state or province. By establishing an account, you can access the instructor resources for your licensed titles on our site. If you establish an account with us, we will process information about your activity on our site, such as displaying when your licenses expire.

Sharing and Use of Information

All information we collect is used solely for educational purposes. We use the information described above to provide you access to our services, to communicate with you, to manage and improve our site, and for security purposes. As noted above, we do not sell the information we collect. Additionally, except as provided below, we will not share, or disclose information we collect from or about you.

Our sites use Google Analytics. Google Analytics places a cookie on your web browser and collects information such as IP address, the identity of Internet Service Provider, browser type, operating system, the referring web page, and the pages visited while on our site. It does not collect names or other identifying account information. We use this information to diagnose problems and to improve and administer the site.

We will share information, if required, to comply with the law or to protect ourselves against third party claims.

Data and System Security

We take industry-accepted administrative, technical, and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of user and account data. No data transmission or storage over the internet is 100% secure. While we use best-practice industry standard security measures to protect personal information, we cannot promise or guarantee absolute security.

In the event of a data breach, which means an unauthorized access, disclosure, alteration, or use of user or account data (or circumstances that could have resulted in such unauthorized access, disclosure, alteration, or use) we promptly institute the following: (1) notify the school/district by telephone and email as soon as practicable, but no later than twenty-four hours after we become aware of the data breach; (2) provide the school/district with the name and contact information for a B.E. Publishing employee who shall serve as our primary security contact; (3) assist the school/district with any investigation, including interviews with our employees and review of all relevant records; (4) assist the school/district with any notification the school/district deems necessary related to the security breach; and (5) immediately engage and implement any necessary administrative, technical, and physical measures to protect systems and data.

Children's Information – FERPA and COPPA Compliance

Students do not create personal accounts to access resources on eReadiness.com. Therefore, children under the age of 13 are not able to create their own account on eReadiness.com even with consent from a parent, legal guardian, or teacher. In fact, teachers with an eReadiness.com account, or school administrators with an eReadiness.com account, are the ones responsible for directing students to the eReadiness.com site to access a title's student resources.

Information such as IP address, the identity of their Internet Service Provider, browser type, operating system, the site that brought them to our site, and the pages visited while on our site will still be collected, via a session cookie for performance management, from children who use the site without creating an account.

This information is lost and unsaved upon exiting the site. If you are the parent, legal guardian, or teacher of someone under the age of 13 who may have created an account and provided us with information without your knowledge or consent, please contact us at support@eReadiness.com to have this information removed. If you know of anyone under the age of 13 who may have provided us with information, please report it to us at support@eReadiness.com.

Children may access the open student resources on eReadiness.com provided that their school has complied with its responsibilities under the Family Educational Rights and Privacy Act ("FERPA") and the Children's Online Privacy Protection Act ("COPPA"). For parental and legal guardian rights, see specific section below. Contained within this privacy policy we provide each school with all the notices required under COPPA.

Please refer to the "Information We Collect" section for more information on the information we collect from children. eReadiness.com does not allow children to make this information publicly available.

Parent's Rights

Parents have the right to review and request that eReadiness.com delete any personal information that the site has collected and retained about their child. If you would like to request that we delete any personal information we may have about your child or to request no further collection of personal information from your child, please contact us at support@eReadiness.com, call us at 1-888-781-6921 or write to us at:

B.E. Publishing, Inc.
P.O. Box 8558
Warwick, RI 02888

Do Not Track Signals

Like most web pages, we do not respond to Do Not Track signals.

California Residents

To reiterate, we do not share, sell, or otherwise give away private information to anyone. But know that as a California resident you have the right to request that we tell you the categories of personal information we collect about you, where we get that information from, why we collect your personal information, who we share your information with, and what pieces of information we have collected about you. You also have the right to request that we tell you the types of businesses we share your information with, and what type of personal information we share with them. You have the right to request that we delete any of your information we have collected. You can submit any of the above requests at support@eReadiness.com.

We cannot discriminate against you for exercising your rights under the California Consumer Privacy Act ("CCPA"). Examples of discrimination would include denying you our services, charging you a different price, providing a different level of quality, or even suggesting you might receive a different price or a worse product.

California Residents – Sale of Children’s Information

To reiterate, we do not share, sell, or otherwise give away private information to anyone. So, if you are between the ages of 13 and 16 and live in California, we could not sell your information unless you consented. If you are a child under the age of 13, we could not sell your information without parental consent.

If you are the parent, legal guardian, or teacher of someone under the age of 13 who may have created an account and provided us with information without your knowledge or consent, please contact us at support@eReadiness.com to have this information removed.

Retention and Deletion of Data

Once an account’s license is cancelled or expires, all account information, including any Personally Identifiable Information that may have been collected relating to a child’s use of the service, is securely archived for one year. One year after the cancellation or expiration of an account’s license, all Personally Identifiable Information within an account will be securely deleted.

Links to Other Sites

If you click on a link to a third-party site, you will be taken to websites we do not control. This policy only applies to the practices of eReadiness.com. We are not responsible for these third-party sites. Our site may also serve third party content that contains their own cookies or tracking mechanisms.

International Visitors

If you do not live in the United States, know that information we collect will be transferred to and processed in the United States. By using our site, you consent to the collection, transfer, processing, and storage of your information in the United States.

Questions or Concerns

If you have any questions about this Privacy Policy, please feel free to email us at support@eReadiness.com or write to us at:

B.E. Publishing, Inc.
P.O. Box 8558
Warwick, RI 02888

Policy Changes

eReadiness.com may update this Privacy Policy from time to time. We will notify you of any material changes to our Policy as required by law. We will also post an updated copy on our website. Please check our site periodically for updates.