wnyric
www.wnyric.org
Erie 1 BOCES Education Campus • 355 Harlem Road • West Seneca, NY 14224-1892
erie boces

EXHIBIT D

DATA SHARING AND CONFIDENTIALITY AGREEMENT

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

1. Purpose

(a) This Exhibit supplements the Master License and Service Agreement ("MLSA") to which it is attached, to ensure that the MLSA conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Exhibit consists of the terms of this Data Sharing and Confidentiality Agreement, a copy of Erie 1 BOCES' Parents Bill of Rights for Data Security and Privacy signed by the Vendor, and the Supplemental Information about the MLSA that is required to be posted on Erie 1 BOCES' website.

(b) To the extent that any terms contained within the MLSA, or any terms contained within any other Exhibits attached to and made a part of the MLSA, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In the event that Vendor has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the MLSA, to the extent that any term of the TOS conflicts with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

2. Definitions

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

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Vendor receives from a Participating Educational Agency pursuant to the MLSA.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Vendor's Product.

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

3. **Confidentiality of Protected Data**

(a) Vendor acknowledges that the Protected Data it receives pursuant to the MLSA may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Vendor will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and Erie 1 BOCES's policy on data security and privacy. Vendor acknowledges that Erie 1 BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, but that adoption may not occur until a date subsequent to the effective date of the MLSA. Erie 1 BOCES will provide Vendor with a copy of its policy as soon as practicable following adoption., and Vendor and Erie 1 BOCES agree to engage in good faith negotiations to modify this Data Sharing Agreement to the extent necessary to ensure Vendor's continued compliance with Section 2-d.

4. **Data Security and Privacy Plan**

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

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

(a) In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Sharing and Confidentiality Agreement, consistent with Erie 1 BOCES' data security and privacy policy, Vendor will: Review its data security and privacy policy and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this Data Sharing and Confidentiality Agreement. In the event Vendor's policy and practices are not in conformance, the Vendor will implement commercially reasonable efforts to ensure such compliance, which the Parties agree does not include R&D development beyond Vendor's current resources.

(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, which includes Vendor's standard technical, operational, and physical safeguards in protecting all customer data.

(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*] __X____will _____will not utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the MLSA. In the event that Vendor engages any subcontactors, assignees, or other authorized agents to perform its obligations under the MLSA, it will require such subcontactors, assignees, or other authorized agents to execute written agreements as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(f) Vendor will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Vendor will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Vendor will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the MLSA is terminated or expires, as more fully described in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

5. **Additional Statutory and Regulatory Obligations**

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

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist Vendor in fulfilling one or more of its obligations under the MLSA.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of Vendor using the information to carry out Vendor's obligations under the MLSA, unless:

   (i) the parent or eligible student has provided prior written consent; or
   (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in Erie 1 BOCES' "Supplemental Information about the MLSA," below.

(g) Provide notification to Erie 1 BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by Vendor or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Subject to the terms and conditions of this Agreement, 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. <u>Notification of Breach and Unauthorized Release</u>

(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 if available at the time of notification, including but not limited to: a description of the incident, the date of the incident, the date Vendor discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Vendor representatives who can assist affected individuals that may have additional questions.

(d) Vendor acknowledges that upon initial notification from Vendor, Erie 1 BOCES, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor shall not provide this notification to the CPO directly. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by Erie 1 BOCES, Vendor will promptly inform Michelle Okal-Frink or her designees.

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

EXHIBIT D (CONTINUED)

ERIE 1 BOCES

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York State Education Law Section 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 using the form available at the following website http://www.nysed.gove/data-privacy-security/report-improper-disclosure. submitted .

BY THE VENDOR:

DocuSigned by:
Scott Virkler
Signature DB07F5614E9A445...

Scott Virkler
Printed Name

Chief Operating Officer
Title

□/21/2020
Date

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
BETWEEN
ERIE 1 BOCES AND ILLUMINATE EDUCATION, INC.

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

FastBridge
FastBridge SEL
FastFlix

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

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

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

Duration of MLSA and Protected Data Upon Expiration:

- The MLSA commences on July 1, 2020 and expires on June 30, 2023.
- Upon expiration of the MLSA without renewal, or upon termination of the MLSA prior to expiration, Vendor will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Vendor or its assignees or subcontractors or other authorized persons or entities to whom it has disclosed Protected Data.
- 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: Unless self-hosted by a Participating Educational Agency, 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 standard 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.

illuminate education

Data Security & Privacy Plan

Illuminate is a web-based "all-the-data" system used by K-12 schools and districts to access student data. Teachers or administrators login to Illuminate and view student demographic and achievement data. Data is the primary element of the system and, as such, data security is paramount to Illuminate. This document will explain how Illuminate protects and values all of the data being utilized through the Illuminate systems.

Family Education Rights and Privacy Act (FERPA)

Illuminate adheres to all rules and regulations related to the protection of confidential student information as described in FERPA and District student confidentiality Board Policies. Illuminate's extensive permissions system ensures that staff members can only access features and student records appropriate to their positions.

Permissions

Illuminate has implemented a comprehensive permission system that allows clients to establish precise access rights over software features and district data. This includes field-level permissions for sensitive data. All permissions are managed through an easy-to-use online web interface. The permission structure in Illuminate is paramount in enforcing FERPA compliance.

Data Access

User access via the web UI

Only users who have been authorized by the school district may login to the Illuminate system. Illuminate offers third party authentication (Active Directory, Google, etc.) integration options to clients who are leveraging the tools in order to bolster login security. All authorized users are provisioned their own individual account, and must provide appropriate credentials with every login. Additionally, users are automatically logged out of the system after a period of inactivity.

Direct database access

At the client's request, direct read-only access to the Illuminate database can be granted to specific administrative users. This read-only access provides access only to the client database. All data is transmitted via SSL. The database user is given specific credentials to login to the database and access to the database is restricted to a client-specified IP address.

API access

Illuminate offers an open API to external parties at the request of clients. Prior to establishing the API access, the external party's data usage plan is evaluated by Illuminate staff. All API consumers are vetted by Illuminate. Once an API partner has been provided secure API access, the actual access to a district's installation is controlled by the district. API access is controlled by two levels of security -- first with API consumer tokens, and second with client administered and permissioned user access controls.

SFTP file transfers

Where routine file transfers are necessary for data imports and exports, only authorized users are granted restricted access to an Illuminate SFTP server. Secure FTP is used to ensure that sensitive data is encrypted in transit.

Software Security

All Illuminate data is stored securely and encrypted during transmission. The security at the software level includes secure access to the Illuminate API, single tenancy to ensure data privacy across clients, and transport layer security.

Secure API Access

API access is controlled by two levels of security -- first with API consumer tokens, and second with client administered and permissioned user access controls. Every time data is accessed via the API, both the consumer token and the client access keys are evaluated for security.

Single Tenancy

Each district's data is stored in its own dedicated database. Data is never co-mingled with data from other Illuminate clients. File transfers are also sent to district-specific locations to ensure that districts do not have visibility into each other's data.

Transport Layer Security

All Illuminate web traffic is encrypted over the wire via SSL. Firewalls are used to limit access to only essential services. Direct database access for district technical staff is managed by Illuminate, and all database traffic is also encrypted in transit via SSL.

Data Center and Cloud Provider

Illuminate products hosted in the Google Cloud Platform benefit from the same security precautions Google uses for its own products. Physical data centers include multi-layered security featuring camera and physical monitoring, credential scanning, and biometric checks.

https://cloud.google.com/security/overview/whitepaper

Illuminate also leverages a cloud-based data center at Amazon Web Services.

Google data center security includes:

- Key card access
- Biometric scanners
- Double mantrap entry
- 24x7x365 perimeter and interior recorded video surveillance
- 24x7x365 in-house security guards
- Locked server cabinets

Google data center certifications include:

- NIST SP 800–61
- ISO 50001

Backup and Disaster Recovery

Illuminate maintains both onsite and offsite backups for all client databases, allowing us to store and retrieve data anytime. Backups are shipped offsite nightly, and are encrypted at rest to prevent data theft. In the event of a catastrophic data center failure, we can retrieve data that is at most 24 hours old.

Audit Logs

Logging occurs at multiple levels within the system. We maintain a log in the system database that records data-changing operations. Page accesses can also optionally be recorded in a flat file showing the page accessed, the user performing the access, and the date/time of the access. Certain areas of the system, such as official student grades, also have their own logging features that track more detailed information about each transaction.

Conclusion

Illuminate believes in students and educators and takes the security of their data very seriously. Illuminate has gone to great lengths to ensure that data is secure physically, in all methods of data transit, and via the software application. Additionally, all Illuminate staff is trained on FERPA and the severe importance of data security. Users of the Illuminate system can use the system confidently, knowing that Illuminate deeply values data security.