

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. In order to streamline procurement, Vendors will maintain a single statewide agreement. This means the same products would not be found on other state wide consortium agreements including 6360 Instructional Technology Consortium, 7710 RIC Consortium, 5877 Distance Learning Consortium, or 6316 DREAM.

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: [NoRedInk Data Security 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*] ☒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 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:

DocuSigned by:

*Emile Bjerkholt*71DAA46309BE470...
SignatureEmile Bjerkholt**Printed Name**Chief of Staff**Title**7/13/2023**Date**

EXHIBIT D (CONTINUED)

SUPPLEMENTAL INFORMATION

 ABOUT THE MASTER LICENSE AND SERVICE AGREEMENT
 BETWEEN
 ERIE 1 BOCES AND NOREDINK CORP.

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

NoRedInk

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: NoRedInk Corp. will be responsible for the actions or omissions of such subcontractors as if it had acted or failed to act, and will only utilize subcontractors which maintain data protection and security policies consistent with NoRedInk Corp.’s obligations under this Exhibit

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.

NoRedInk Data Security Plan

References

NoRedInk is ISO 27001 certified (#122203)
Privacy policy (<https://www.noredink.com/privacy>)
Copyright policy (<https://www.noredink.com/copyright>)
Terms of Service (<https://www.noredink.com/terms>)

Hosting and Access Control

Hosting

Our application is hosted through Amazon Web Services (AWS).

Hardware security

Only Amazon administrators have physical access to our hardware, and Amazon has their own procedures to ensure the security of that hardware.

Access Control

NoRedInk maintains an Information Security Management System (ISMS). We do so currently via 3rd party. Our product service resides on AWS. As an ISMS, AWS is certified as compliant with ISO 27000. (https://d1.awsstatic.com/certifications/iso_27001_global_certification.pdf)

Access to our production infrastructure such as applications servers is permission controlled through AWS Identity and Access Manager (IAM) (<https://aws.amazon.com/iam>) policies. We require engineers to upload ssh access tokens and are able to revoke access centrally for individuals. Password only authentication to these hosts is disabled and access is only possible through use of the access tokens.

Database access is limited to users with these tokens by ssh tunnelling through an infrastructure host. There is read access to data in the database for reporting using metabase.io, this access is limited by NoRedInk google credentials.

Logs

We use AWS CloudTrail, which gives logs about user access and infrastructure changes. We use GoogleApps, which gives us logs about user access. We have logs from our application servers, database servers, and load balancers. Logs are retained for 90+ days. Only 3rd Party (AWS / Google) and key internal administrative staff have access to these logs.

Data Policies

Compliance

We comply with the following laws concerning the protection of student personally identifiable information, including educational records: the Family Educational Rights and Privacy Act (“FERPA”), Children’s Online Privacy Protection Act (“COPPA”), and New York State Education Law Section 2-D.

Child Friendly Policies, Terms and Conditions

Our policies and terms are written in a non-legaleze friendly format. In addition, based upon our COPPA alignment, underage and/or minor students must have parental consent to utilize our services.

Our privacy policy (<https://www.noredink.com/privacy>) makes it clear the age restrictions for the use of the NoRedInk service, including parental consent for underage children.

Use of Data

Our privacy policy (<https://www.noredink.com/privacy>) makes it clear that we will not rent or sell PII. We do share de-identified data with 3rd party services for analysis in support of product maintenance and improvement.

We don’t serve advertising within the product but we do use the following services for analysis in support of product maintenance and improvement: Google Analytics, MixPanel, Customer.io, Inspectlet, Rollbar, and Bugsnag.

User Access to Data

We do not provide unnecessary visibility of other users, and there is no public-facing or in-solution browsable user profile for students or teachers.

Students can only access information relating to their own account, their own scores on practice assignments, quizzes, or their own writing sections.

Teachers can access information relating to their own account as well as see the scores and submissions for their student’s work on the site.

Facilitator access upon request gives school based admin access to all teacher and student accounts in the building.

Data Ownership

Our terms of service (<https://www.noredink.com/terms>) describe our policy of ownership of user submissions. All user submissions belong to the user, however the user grants NoRedInk a license to translate, modify (for technical purposes, for example making sure the content is viewable on an iPhone as well as a computer) and reproduce such user submissions, in each case to enable us to operate the Services. This is a license only – ownership in user submissions is not affected.

We are in compliance with CCPA, which requires we have a means to provide and remove a user’s data from our system. At any time, the client may request a copy of their data, or a request for deletion, directly from NoRedInk by submitting a written request via Privacy Request Form (<https://preferences.noredink.com/privacy>).

Data Storage and Security

Data Location

All customer data is stored in the United States.

Data Backup and Recovery

We use AWS processes for data backup and recovery. For Amazon RDS, we maintain storage across multiple availability zones. We have database replicas which can quickly replace our master RDS database in the case of a failure. In addition, we maintain a 30-day backup on Amazon RDS.

Data Encryption

All client to server data is transmitted with TLS 1.2 over HTTPS. At rest, we utilize Amazon RDS's at-rest encryption solution, Transparent Data Encryption. Passwords are further encrypted at rest using the bcrypt function.

In addition, it is our policy to avoid storing any personal data on employee devices.

Web Environment Security

We store cookies on user's computers, we do not store credentials that could be used for re-authentication. Cookies are encrypted and signed, and are sent with the flags 'secure' and 'http-only' to prevent the most common attacks. We have tools in place to monitor abnormal system behavior (NewRelic, Rollbar, etc.) but do not use a traditional Intrusion Prevention System to identify problematic network activity.

We also use backend frameworks with built in input validation, including SQL sanitization to prevent SQL injection, and string sanitization to prevent XSS. All of our forms automatically include an authenticity token to prevent CSRF.

System Security

Security Updates

The engineering team maintains a listing of the "sunset dates" of security support of all external software dependencies, and prioritizes updating those dependencies in advance of any sunset of security support.

In addition, the engineering department maintains a weekly "security rotation," supported by automated detection of dependency security updates (via Dependabot). This results in security updates typically being incorporated into the system within 1 week.

User Account Security

All users of the application require a password-protected login in order to authenticate. Teachers and students can register with a unique username and a password, or use Google SSO or Clever SSO.

Because we do not require students to provide an email, we cannot use the traditional password-reset-via-email mechanism in the case of a student forgetting their password. For this use case, teachers have the ability to reset the passwords of their students.

User credentials are encrypted, as all data, using our standard encryption in transit and at rest requirements. In addition, passwords are further encrypted at rest using the bcrypt function. We do not store or transmit a user password without encryption.

Third Party Services and Subcontractors

We only partner with third party services and subcontractors whose privacy policies are consistent with the obligations within our privacy principles (<https://www.noredink.com/privacy>). We 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 specific customer, state and federal laws and regulations.

Incident Management and Response

We have 24/7 on call support for incident response. Two-to-three engineers are on call each week. We use several application monitoring services (NewRelic, Datadog, Rollbar, Bugsnag), configured to alert our on-call engineers via Slack in the case of a possible incident. All alerts must be investigated, and all fires must be addressed immediately.

We maintain, and continue to expand, a library of on call response playbooks which detail both how to respond and relevant surrounding context, for a variety of possible incident scenarios. We aim to link each of our alerts to the relevant playbook to facilitate a rapid incident response.

In addition, all fires require detailed write-ups of the events of the incident and investigation, any root cause analysis, and next steps. These write-ups are reviewed by key stakeholders, and next steps are recorded and prioritized by the appropriate teams.

In the case of a data breach, our current practice is to notify a client within 48 hours of the recognition of a data breach.

Data Transition and Secure Destruction

Upon expiration or termination of the Contract or Agreement, NoRedInk shall:

- 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 and remove it from any archival databases within 30 days of expiration.

Training

NoRedInk provides periodic security and privacy training to those of its employees and individual consultants who operate or have access to the system. NoRedInk contracts with Vanta for employee training that covers the following topics: general cybersecurity, reporting suspicious activity, passwords, password managers, MFA, malware, ransomware, phishing, mobile security, cloud security threats, policy violations, data classification and data privacy.