

PRATTSBURGH CENTRAL SCHOOL DISTRICT DATA PRIVACY AGREEMENT

PRATTSBURGH CENTRAL SCHOOL DISTRICT

and

NoRedInk

This Data Privacy Agreement ("DPA") is by and between the Wellsville Central School District ("EA"), an Educational Agency, and NoRedInk ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

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

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

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

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated [Insert Date] ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education’s Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New

York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

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

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

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

8. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. Data Return and Destruction of Data.

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

10. Commercial or Marketing Use Prohibition.

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

11. Encryption.

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

12. Breach.

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

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

Name: Prattsburgh Central School District

Title: Data Privacy Officer, Kory Bay

Address: 1 Academy Street

City, State, Zip: Prattsburgh, NY 14873

Email: bayk@prattsburghcsd.org

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its’ Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

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

15. Termination.

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

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

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

2. Bill of Rights for Data Privacy and Security.

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

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

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

2. Execution.

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


EDUCATIONAL AGENCY	CONTRACTOR
BY: [Signature] <i>Kristina McCracken</i>	BY: 
[Printed Name] Kristina McCracken	Stephen Gardner
[Title] Data Protection Officer Assistant	VP of Sales & Success
Date: 02/14/23	Date: 8/5/2022

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

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

1. A student’s personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student’s name or identification number, parent’s name, or address; and indirect identifiers such as a student’s date of birth, which when linked to or combined with other information can be used to distinguish or trace a student’s identity. Please see FERPA’s regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student’s education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education’s Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student’s identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints may be submitted to the DPO, Kory Bay via mail: Prattsburgh CSD, Data Privacy Officer, 1 Academy Street, Prattsburgh, NY 14873, by emailing dpo@prattsburghcsd.org , or by calling 607-522-6211. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.


CONTRACTOR	
[Signature]	
[Printed Name]	Stephen Gardner
[Title]	VP of Sales & Success
Date:	8/5/2022

EXHIBIT B

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

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

Name of Contractor	NoRedInk
Description of the purpose(s) for which Contractor will receive/access PII	Use and reproduction of the data to the extent necessary to provide, maintain, and improve Contractor’s services. During and after the term, use and analysis of data about the use of the service provider’s services in order to maintain and improve those services
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date <u>8/5/2022</u> Contract End Date _____
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA’s option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA’s written request.

Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>Only the administrators of the cloud infrastructure provider have physical access to the data centers from which our service is hosted; the cloud infrastructure provider maintains security procedures compliant with a variety of US and international standards to ensure physical security of their data centers. It is our policy to prohibit storing any user data on employee devices. Access to the NoRedInk production servers and database is permission controlled. We are able to revoke access remotely for any individual.</p> <p>All end users of the online application require a password-protected login in order to access the application. Teachers and students can register with a unique username and a password, or use Google SSO or Clever SSO.</p> <p>All user data, including login credentials, provided in the use of the online service is encrypted in transmission using HTTPS. User data, including passwords, is encrypted at rest in our database.</p>
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	
[Printed Name]	Stephen Gardner
[Title]	VP of Sales & Success
Date:	8/5/2022

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

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

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	See attached
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	See attached
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	See attached
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	The Contractor ensures that any and all subcontractors, persons or entities that the Contractor may share the Data with abide by the terms of District, State and national privacy agreements and frameworks.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	See attached
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Data is deleted from the active database when requested by the District, or when Contractor's agreement with the District ends.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Data is permanently overwritten in Contractor's archival database 30 days after removal/deletion from the active database. Certification is provided in writing upon request by the District.

8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	See attached.
---	---	---------------

NoRedInk Data Security Plan

References

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 Children's Online Privacy and Protection Act (COPPA) and California Consumer Protection Act (CCPA).

Child Friendly Policies, Terms and Conditions

Our policies and terms are written in a non-legal 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 sunsetting 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

We only partner with third party services whose privacy policies are consistent with the obligations within our privacy principles (<https://www.noredink.com/privacy>).

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.

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.