



DATA SECURITY AND PRIVACY PLAN

WHEREAS, the Liverpool Central School District (hereinafter “School District”) and NoRedInk Corp. (hereinafter “Contractor”) entered into an agreement dated 07/12/2023 (hereinafter “Agreement”) for NoRedInk free version (hereinafter “Services”).

WHEREAS, pursuant to the requirements under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

1. During the term of the Agreement, Contractor will implement all state, federal and local data security and privacy requirements, consistent with the School District's Data Security and Privacy Policy in the following way(s)

Please see attached NY state Data Security plan. NoRedInk is ISO 27001 certified (#122203).

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement:

Please see attached NY state Data Security plan. NoRedInk is ISO 27001 certified (#122203).

3. Contractor shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the School District's Parents Bill of Rights for Data Privacy and Security and will comply with same.

- a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.
- b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the “Supplemental Information” appended to the Agreement.
- c. At the end of the term of the Agreement, Contractor will destroy, transition or return, at the direction of the School District, all student data and all teacher and principal data in accordance with the “Supplemental Information” appended to the Agreement.

- d. Student data and teacher and principal data will be stored in accordance with the “Supplemental Information” appended to the Agreement.
- e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided:

Specify date of each training

NoRedInk provides annual training. Training last occurred in Aug 2022 and will be scheduled for the 2023 shortly.

5. Subcontractors (select one): b. Contractor shall utilize subcontractors

- a. Contractor shall not utilize subcontractors.
- b. Contractor shall utilize subcontractors. Contractor shall manage the relationships and contracts with such subcontractors in the following ways in order to ensure personally identifiable information is protected:

NoRedInk only partners with third party services and/or subcontractors whose privacy policies are consistent with the obligations within our privacy principles. Please see attached NY state Data Security plan for more details.

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information:

Procedures, plans or protocols must, at a minimum, specify plans to identify breaches and unauthorized disclosures, and to promptly notify the School District.

Please see attached NY state Data Security plan. NoRedInk is ISO 27001 certified (#122203).

7. Termination of Agreement.

- a. Within 30 days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession; AND
- b. Within days of termination of the Agreement, Contractor shall
 Return all data to the School District using ; OR

Transition all data to a successor contractor designated by the School District in writing using _____.

8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Contractor hereto has executed this Data Security and Privacy Plan as of 07/12/2023.

Contractor: NoRedInk Corp.

Title: Chief of Staff

Date: 07/12/2023

Parents Bill of Rights
Liverpool Central School District

The Liverpool School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, parents and eligible students can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any commercial purpose.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.
3. State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of a student's PII, 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 NYSED is available for public review and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be submitted to NYSED online, 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.
6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.
8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Liverpool School District has entered into agreements with certain third-party contractors.

Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
3. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);
4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
6. Address how the data will be protected using encryption while in motion and at rest.

Daniel P Farsaci

Liverpool Administrator Signature

Daniel Farsaci

Liverpool Administrator Printed Name

07/13/2023

Date

Emile Bierkholt

Representative Signature

Emile Bierkholt

Representative Printed Name

07/12/2023

Date



Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM – ISO/IEC 27001:2013

The Certification Body of Prescient Security, LLC hereby certifies that the following organization operates an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2013

NoRedInk Corp.

548 Market St, PMB 66984, San Francisco, CA 94104

for the following scope of registration

The scope of the ISO/IEC 27001:2013 certification is limited to the Information Security Management System (ISMS) supporting **NoRedInk Corp.**'s Software-as-a-Service (SaaS), Web application products in accordance with the Statement of Applicability version 2.0 dated 01/25/2023.

CERTIFICATE NUMBER: 122203



PRESIDENT
SECURITY



MSCB-267

Authorized By:

Fabrice Mouret

CEO, Prescient Security, LLC
1211 Main Street Suite 2
Salmon, ID 83467, USA
www.prescientsecurity.com

Issue Date
March 31, 2023

Registration Date
March 31, 2023

Expiration Date
October 31, 2025

Certificate Version
1.8

CONDITIONS & LIMITATIONS:

1. The aforementioned organization has a perpetual responsibility to maintain compliance with ISO/IEC 27001:2013 during the period of certification.
2. This certificate is subject to the satisfactory completion of annual surveillance by Prescient Security, LLC.
3. ISO/IEC 27001:2013 compliance audits are not designed to detect or prevent criminal activity or other acts that may result in an information security breach. As such, this certification should not be construed as a guarantee or assurance that an organization is unsusceptible to information security breaches.
4. The information in this document is provided "AS IS", without warranties of any kind. Prescient Security, LLC. expressly disclaims any representations and warranties, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose.
5. This certificate is the property of Prescient Security, LLC and is bound by the conditions of the contract. The authenticity of this certificate can be validated by contacting Prescient Security. For more information about the validity of this certificate, please contact isoteam@prescientsecurity.com

As of 2023, NoRedInk is ISO 27001 certified (#122203)

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 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-legalese 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 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.