

ADDENDUM TO THE SUPPLEMENTAL AGREEMENT BETWEEN SAG HARBOR UNION FREE SCHOOL DISTRICT AND NOREDINK

Sag Harbor Union Free School District (hereinafter the “Client”) and NoRedInk Corp. (hereinafter the “Company” or “NoRedInk”), agree that this Addendum between Client and NoRedInk (“Addendum”) is hereby incorporated and made a part of the Supplemental Agreement (hereinafter collectively the “Agreements”). If any conflicts or inconsistencies exist between or among this Addendum and the Agreements, the Client and Company agree that the provisions of this Addendum shall supersede and prevail. Client and Company may be referred to herein individual as the “Party” and collectively as the “Parties”.

1. Notwithstanding the foregoing, or anything to the contrary contained in the Agreements, the provisions of NoRedInk’s licensing terms located at <https://www.noredink.com/terms> and NoRedInk’s Privacy Policy located at <https://www.noredink.com/privacy> shall supersede and prevail over any conflicting or inconsistent terms found in the Agreements.
2. Notwithstanding anything to the contrary contained in the Agreements, the Termination of the Agreements and this Addendum shall only occur as follows: i) immediately after written notice by either Party upon material breach of the Agreements or Addendum, (ii) upon expiration of the license for use of the NoRedInk software; (iii) by mutual, written agreement of the Parties.
3. Any indemnification under the Agreements shall be limited to the greater of: i) the fees paid by the Client to the Company over the twelve month period preceding the incident giving rise to the claim for indemnification, OR ii) one thousand dollars.
4. Should there be a conflict in the governing law provisions of the terms and privacy policy of NoRedInk and the Agreements, the Agreements shall prevail to so long as the choice of law therein reflects the jurisdiction in which the Client is located.
5. To the extent that a data security plan is required by the Client, the contents and provisions of NoRedInk’s Data Security Plan, attached hereto as Exhibit A, shall be deemed sufficient and acceptable to the Client.
6. The sale of a majority interest in the Company or the sale of all or substantially all of the assets of the Company shall not be considered any assignment under the

Agreements and therefore would not require the approval of the Client to be effective.

CLIENT:

Sag Harbor Union Free School District

Signature:  _____

Name: Jeff Nichols

Title: Superintendent of Schools

Date: January 23, 2024

COMPANY:

NoRedInk Corp.

Signature:  _____

Name: Blake Sipek

Title: Chief Financial Officer

Date: 11/08/23

Exhibit A
NoRedInk's Data Security Plan



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



PRESCIENT
SECURITY



Authorized By:

Fabrice Mouret

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

MSCB-267

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-legalize 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.

**Supplemental Agreement between the
Sag Harbor Union Free School District
and
NoRedInk Corp.**

Supplemental Agreement dated this **8** day of **November, 2023** between the Sag Harbor Union Free School District (the “District”), located at 200 Jermain Avenue, Sag Harbor, New York 11963, and **NoRedInk Corp.** (the “Contractor”) located at **548 Market St, PMB 66984, San Francisco, California 94104**

WHEREAS, the District and Contractor have entered into a contract or other written agreement (hereinafter the “Agreement”) whereby the Contractor may receive Student Data or Teacher or Principal Data, as those terms are defined in Education Law §2-d; and

WHEREAS, the District and Contractor wish to enter into an agreement in order to comply with Education Law §2-d (hereinafter “Supplemental Agreement”).

NOW THEREFORE, in consideration of the mutual promises below, the District and Contractor agree as follows:

1. Defined Terms: Unless otherwise indicated below or elsewhere in this Supplemental Agreement, all capitalized terms shall have the meanings provided in Education Law §2-d and Section 121.1 of the Regulations of the Commissioner of Education (hereinafter “Regulations”).
 - a. “Educational Agency” shall generally have the same meaning as the term Educational Agency at Education Law §2-d(1)(c) and Section 121.1(f), and in reference to the party to this Agreement shall mean the Sag Harbor Union Free School District
 - b. “Third Party Contractor” shall mean any person or entity, other than an Educational Agency, that receives Student Data or Teacher or Principal Data from an Educational Agency pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs.
 - c. “Student” means any person attending or seeking to enroll in an Educational Agency.
 - d. “Student Data” means Personally Identifiable Information of a “Student.”
 - e. “Eligible Student” means a Student who is eighteen years or older.
 - f. “Parent” means a parent, legal guardian, or personal in parental relation to a Student.
 - g. “Building Principal” or “Principal” means a building principal subject to annual performance evaluation review under Education Law §3012-c.
 - h. “Classroom Teacher” or “Teacher” means a teacher subject to annual performance evaluation review under Education Law §3012-c.

i. “Teacher or Principal Data” means 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.

j. “Personally Identifiable Information” shall have the following meanings:

i. As applied to Student Data, shall mean Personally Identifiable Information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA)

ii. As applied to Teacher or Principal Data, shall mean Personally Identifiable Information as that term is defined in Education Law §3012-c.

2. The District has developed the Parents Bill of Rights for Data Privacy and Security, the terms of which are applicable to the Agreement between the District and Contractor and are incorporated into this Supplemental Agreement. The Parents Bill of Rights for Data Privacy and Security states:

Parents’ Bill Of Rights For Data Privacy And Security

The Sag Harbor Union Free School District is committed to protecting the privacy and security of student, teacher, and principal data. Pursuant to New York State Education Law §2-d, parents, legal guardians, and persons in parental relation to a student are entitled to certain rights with regard to their child’s personally identifiable information. The Sag Harbor Union Free School District is hereby informing the community of the following rights:

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 educational records maintained by the Sag Harbor Union Free School District.
3. State and Federal Laws protect the confidentiality of personally identifiable student 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 New York State is available for review at the following website:

<http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>

The list may also be made available by writing to:

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 to:

Scott Fisher, Data Privacy Officer
Sag Harbor Union Free School District
200 Jermain Avenue, Sag Harbor, New York 11963
(631) 725-5300 x 455 Email: dpo@sagharborschools.org

OR

Chief Privacy Officer
New York State Education Department
89 Washington Avenue, Albany, New York 12234
Email: CPO@mail.nysed.gov

Supplementary Information Regarding Third-Party Contractors:

In the course of complying with its obligations under the law and providing educational services, the Sag Harbor Union Free School District has entered into agreements with certain third-party contractors. Pursuant to such agreements, third-party contractors may have access to student data and/or teacher or principal data. Each contract the Sag Harbor Union Free School District enters into with a third-party where the contractor receives student data and/or teacher or principal data will include information addressing the following:

- The exclusive purposes for which the student data and/or teacher or principal data will be used.
- How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data and/or teacher or principal data with, if any, will abide by data protection and security requirements.
- When the agreement expires and what happens to the student data and/or teacher or principal data upon expiration of the agreement.
- If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or the teacher or principal data that is collected; and
- Where the student data and/or teacher or principal data will be stored, and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

Third-party contractors are also required to:

- Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data and/or teacher or principal data;

- Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
- Not use educational records for any other purpose than those explicitly authorized in the contract;
- Not disclose personally identifiable information to any other party (i) without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
- Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
- Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law §2-d;
- Notify the Sag Harbor Union Free School District of any breach of security resulting in an unauthorized release of student data and/or teacher or principal data, in the most expedient way possible and without unreasonable delay;
- Provide a data security and privacy plan outlining how all state, federal and local data security and Privacy contract requirements will be implemented over the life of the contract;
- Provide a signed copy of this Bill of Rights to the Sag Harbor Union Free School District thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

This Parents' Bill of Rights for Data Privacy and Security is subject to change based on regulations of the Commissioner of Education and the New York State Education Department's Chief Privacy Officer, as well as emerging guidance documents.

3. As required by Education Law §2-d(3)(c) and Section 121.3 of the Regulations, the District has developed the following "supplemental information" for the Agreement with the Contractor:

- a. Student Data and/or Teacher or Principal Data which the Contractor comes into possession in the course of the performance of its Agreement with the District should not be germane to and thus should not be used for any purpose by the Contractor. Such Data that comes into the possession of the Contractor must be protected in accord with Education Law §2-d and in accord with the Parents Bill of Rights for data Privacy and Security (Exhibit "A").
- b. The Contractor will ensure that any and all subcontractors, persons or entities that the Contractor may share the Student Data and/or Principal or Teacher Data with will abide by the terms of the Agreement, this Supplemental Agreement, the Parents Bill of Rights for

data Privacy and Security and/or the data protection and security requirements set forth in Education Law §2-d.

c. When the Agreement terminates between the District and the Contractor, the Contractor shall return to the District or, if agreed to by the District, destroy the remaining Student Data and/or Principal or Teacher Data that the Contractor still maintains in any form.

d. Any challenges concerning the accuracy of Student Data and/or Principal Data shall be handled directly between the District and the Parent, Student, Eligible Student, Teacher or Principal. The Contractor agrees to abide by the outcome of such challenges and make any corrections and/or changes to the applicable Student Data and/or Principal or Teacher Data as determined by the District.

e. The District and the Contractor hereby agree that the Student Data and/or Principal or Teacher Data shall be stored in the following manner: The Contractor shall maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of the personally identifiable student information in its custody by using all reasonable protections available to the Contractor including but not limited to encryption technology while such data is in motion or in its custody. In order to further outline the methods of storage and protection of Student Data and/or Principal or Teacher Data Contractor shall provide a data security and privacy plan to the District within 30 days of the execution of this agreement.

4. As required by Education Law §2-d(5)(e), the Contractor hereby agrees that any officers or employees of the Contractor, including any subcontractors or assignees, who have access to Student Data or Teacher or Principal Data will have or will receive training on the Federal and New York State laws governing confidentiality of Student Data and/or Principal or Teacher Data prior to receiving access.

5. As required by Education Law §2-d(5)(f), the Contractor hereby agrees that it shall:

a. Limit internal access to education records to those individuals that are determined to have legitimate educational interests;

b. Not use the educational records for any other purposes than those explicitly authorized in the Agreement or this Supplemental Agreement;

c. Except for authorized representatives of the Contractor to the extent they are carrying out the Agreement or this Supplemental Agreement, not disclose any Personally Identifiable Information to any other party:

i. Without the prior written consent of the Parent or Eligible Student; or

ii. Unless required by statute or court order and the party provides a notice of the disclosure to the State Education Department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order.

d. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;

6. Breach and unauthorized release of Personally Identifiable Information:

a. In accordance with Education Law §2-d(6) and Section 121.11 of the Regulations, the Contractor shall be required to notify the District of any breach of security resulting in an unauthorized release of Student Data and/or Principal or Teacher Data by the Contractor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for Student Data Privacy and Security, the data privacy and security policies of the District and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. The District shall, upon notification by the Contractor, be required to report to the Chief Privacy Officer, who is appointed by the State Education Department, any such breach of security and unauthorized release of such data.

b. In the case of an unauthorized release of Student Data, the District shall notify the Parent or Eligible Student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such Student in the most expedient way possible and without unreasonable delay. In the case of an unauthorized release of Teacher or Principal Data, the District shall notify each affected Teacher or Principal of the unauthorized release of data that includes Personally Identifiable Information from the Teacher or Principal's annual professional performance review in the most expedient way possible and without unreasonable delay.

c. In the case of notification to a Parent, Eligible Student, Teacher or Principal due to the unauthorized release of student data by the Contractor, or its subcontractors or assignees, the Contractor shall promptly reimburse the educational agency for the full cost of such notification, as required by Education Law §2-d(6)(c).

7. Miscellaneous:

a. The District and Contractor agree that if applicable laws change and/or if the Commissioner of Education implements Regulations which affects the obligations of the parties herein, this Agreement shall be deemed to incorporate such changes as necessary in order for the District and the Contractor to operate in compliance with the amendment or modified requirements under the applicable laws or regulations.

b. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the District to comply with the applicable laws or regulations.

c. Nothing express or implied in this Agreement is intended to confer upon any person other than the District, Contractor and their respective successors and assigns any rights, remedies, obligations or liabilities.

IN WITNESS WHEREOF, the Parties hereto have duly executed this Agreement.

NoRedInk Corp.

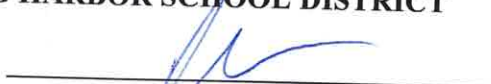
By: 

Print Name: Blake Sipek

Title: Chief Financial Officer

Date: 11/8/23

SAG HARBOR SCHOOL DISTRICT

By: 

Print Name: Jeff Nichols

Title: Superintendent of Schools

Date: 1/23/2024