

This DPA was last revised on March 21, 2020.

Data Protection Addendum for NoRedInk Hosted Service

This Data Protection Addendum (“DPA”) forms part of the Master Service Terms located at <https://www.noredink.com/master-services-terms> and the Order Form (together, the “**Agreement**”), entered into by and between the Client and NoRedInk Corp. (“NoRedInk”), pursuant to which Client accesses, uses and has accessed and used NoRedInk’s Hosted Service (as defined in the Agreement).

This Addendum applies to and takes precedence over the Agreement and any associated contractual document between the parties, such as an order form, statement of work or data protection addendum thereunder, to the extent of any conflict.

1. Definitions

1.1 “**Applicable Data Protection Laws**” means the Family Educational Rights and Privacy Act (“**FERPA**”) at 20 U.S.C. 1232g (34 CFR Part 99), Children’s Online Privacy Protection Act (“**COPPA**”), 15 U.S.C. 6501-6506; Protection of Pupil Rights Amendment (“**PPRA**”) 20 U.S.C. 1232h, AB 1584 (codified at California Education Code § 49073.1), and the Student Online Personal Information Protection Act (codified at California Business and Professions Code § 22584 *et seq.*), any specific state Covered Information protection laws set forth in the table set forth as Exhibit A hereto as of the date set forth in such table as applicable to NoRedInk, and such other state Covered Information protection laws as NoRedInk and Client may agree in writing shall apply.

1.2 “**CCPA**” means the California Consumer Privacy Act, codified at California Civil Code §1798.100 *et seq.*

1.3 “**Covered Information**” means (a) Educational Records and Student-Generated Content provided by Client or generated by the use of the Hosted Service by Client or Users; (b) all elements of Client Data which either identify or can reasonably be used to identify a natural living person; and (c) those elements of Client Data indexed to those elements identified in clause (a). Covered Information excludes any De-Identified Information.

1.4 “**De-Identified Information**” means any information which has been de-identified or aggregated in a manner which renders identification of natural persons infeasible.

1.5 “**Educational Records**” means official records, files and data directly related to a student and maintained by the school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

1.6 “**student**” shall be interchangeable with “pupil” for the purposes of any Applicable Data Protection Laws.

1.7 “**Student-Generated Content**” means materials or content created by a student during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

1.8 Any capitalized but undefined terms herein shall have the meaning set forth in the Agreement.

2. Client Obligations

2.1 Compliance. Client will comply with all Applicable Data Protection Laws in connection with the Agreement.

2.2 Unauthorized Access Notification. Client shall notify NoRedInk promptly of any known or suspected unauthorized access to Client Data, whether or not such access was made with User credentials. Client will reasonably assist NoRedInk in any efforts by NoRedInk to investigate and respond to any unauthorized access.

3. NoRedInk Obligations

3.1 Data Protection Laws: Use Generally. NoRedInk will comply with its obligations under the Applicable Data Protection Laws, provided that as to COPPA or any state law which requires consent or authorization from a parent or guardian for the collection or use of Covered Information, Client is responsible for fulfilling any applicable consent requirement. Without limiting the generality of the foregoing, NoRedInk shall not use or disclose Covered Information received from or on behalf of Client (or its Users) except as permitted or required by the Agreement and this Addendum, as required or expressly permitted by law, or as otherwise authorized in writing by Client. For the purposes of FERPA, NoRedInk shall be considered a School Official, under the control and direction of the Clients as it pertains to the use of Covered Information notwithstanding the above.

3.2 Parent Access. Client shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Covered Information in the student's records, correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. NoRedInk shall respond in a timely manner (and no later than 45 days from the date of the request) to the Client's request for Covered Information in a student's records held by NoRedInk to view or correct as necessary. Subject to NoRedInk's obligations under the CCPA, in the event that a parent of a student or other individual contacts NoRedInk to review any of the Covered Information accessed pursuant to the Hosted Service, NoRedInk shall refer the parent or individual to the Client, who will follow the necessary and proper procedures regarding the requested information.

3.3 Student-Generated Content. If Student-Generated Content is stored or maintained by NoRedInk as part of the provision of the Hosted Service, NoRedInk shall, at the request of the Client or the relevant student, provide a copy thereof to the relevant student or the Client, as applicable, and if such a facility is available, transfer said Student-Generated Content to a separate student account upon termination of the Agreement; provided, however, such transfer shall only apply to Student-Generated Content that is severable from the Hosted Service.

3.4 Third Party Requests. Should a third party, including law enforcement and government entities, contact NoRedInk with a request for data held by NoRedInk in connection with the Hosted Service, NoRedInk shall, if permitted by the law or instrument under which such request is made, redirect the Third Party to request the data directly from the Client. If permitted by the law or instrument under which such request is made, NoRedInk shall notify the Client in advance of a compelled disclosure to a Third Party.

3.5 Employees; Subprocessors. NoRedInk shall require all employees and individual consultants who have access to Covered Information to comply with all applicable provisions of this DPA with respect to the Covered Information. NoRedInk shall be responsible for the actions or omissions of all employees, consultants and subcontractors receiving, accessing or processing Covered Information in connection with the Agreement as if NoRedInk had itself acted or failed to act.

3.6 Use of De-Identified Information. De-identified Information may be used by NoRedInk for the purposes of development, research, and improvement of educational sites, services, or applications, as set forth in the Agreement. NoRedInk will not attempt to re-identify De-identified Information and will not transfer De-identified Information to any party (other than a NoRedInk subcontractor in connection with the provision of the Services or as part of an assignment of the Agreement) unless: (a) the De-Identified Information is either aggregated with other similar data so that neither the identity of Client nor the identity of any natural person can reasonably be derived; or (b) that party agrees in writing not to attempt re-identification.

3.7 Data Availability. NoRedInk will provide the Client with any specified portion of the Covered Information within ten (10) calendar days of receipt of a written request for such Covered Information.

4. Advertising Prohibition.

NoRedInk will not use or sell Covered information to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing or advertising to students or families/guardians; (c) develop a profile of a User or a Student User's family member/guardian, for any commercial purpose other than providing the Service to Client. This section does not prohibit NoRedInk from using Covered Information as set forth in the Agreement and elsewhere in this DPA.

5. Data Security

5.1 Data Security Generally. NoRedInk agrees to abide by and maintain adequate data security measures, consistent with industry standards and good technology practices, to protect Covered Information from unauthorized disclosure or acquisition by an unauthorized person.

5.2 Passwords and Employee Access. NoRedInk shall secure usernames, passwords, and any other means of gaining access to the Hosted Service or to Covered Information, using security standards no less secure than industry standard. NoRedInk shall only provide access to Covered Information to employees, individual consultants or subcontractors that are performing Professional Services or supporting the Hosted Service. Employees and individual consultants with access to Covered Information shall have signed confidentiality agreements regarding said Covered Information. All employees with access to Covered Information shall be subject to criminal background checks in compliance with state and local ordinances.

5.3 Security Protocols. Both parties agree to maintain security protocols that meet industry standards in the transfer, transmission and storage of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so.

5.4 Employee Training. NoRedInk shall provide periodic security training to those of its employees and individual consultants who operate or have access to the system. Further, NoRedInk shall provide Client with contact information of an employee who Client may contact if there are any security concerns or questions.

5.5 Security Technology. NoRedInk shall employ industry standard measures to protect data from unauthorized access, including server authentication and data encryption. NoRedInk shall host Client Data pursuant to the Agreement in an environment using a firewall that is updated according to industry standards.

5.6 Periodic Risk Assessment. NoRedInk will conduct digital and physical periodic (no less than semi-annual) risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner.

5.7 Disposition of Data. NoRedInk shall destroy, delete or de-identify all Covered Information obtained under the Agreement when it is no longer needed for the purpose for which it was obtained, and/or transfer said Covered Information to Client or Client's designee in an industry standard format. During the Term of the Agreement, Client may request partial disposal of Covered Information obtained under the Agreement that is no longer needed. Upon termination of the Agreement, NoRedInk shall destroy, delete, or de-identify all Covered Information obtained under the Agreement by (a) shredding any hard copies of any Covered Information; or (b) secure deletion of electronic copies of Covered Information; or (c) modifying the Covered Information to make it De-Identified Information. The duty to destroy or delete Covered Information shall not extend to Covered Information that has been previously converted to De-Identified Information or placed in a separate account pursuant to the other terms of this DPA.

6. Data Breach.

6.1 Breach Notification. In the event that Covered Information is accessed or obtained by an unauthorized person, NoRedInk shall provide notification to Client within a reasonable amount of time of the incident, and not exceeding forty-eight (48) hours. NoRedInk shall follow the process set forth in this Section 6.

6.2 Notification Structure. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

6.3 Minimum Contents. The security breach notification shall include, at a minimum, the following information:

- (a) The name and contact information of the Client to which the report is made.
- (b) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
- (c) If the information is possible to determine at the time the notice is provided, then either (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(d) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(e) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

6.4 Optional Contents. If feasible, then upon Client’s request, the security breach notification may also include any of the following:

(a) Information about what NoRedInk has done to protect individuals whose information has been breached.

(b) Advice on steps that the person whose information has been breached may take to protect himself or herself.

6.5 Legal Requirements. NoRedInk agrees to adhere to all requirements in applicable state and federal law with respect to a data breach related to the Covered Information, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

6.6 Response Planning. NoRedInk further agrees to have a written incident response plan that reflects good practices and is consistent with industry standards for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Covered Information.

6.7 Other Interactions Regarding Breach. NoRedInk is prohibited from directly contacting parent, legal guardian or students unless expressly requested by Client or required by applicable law (including the CCPA). If Client requests NoRedInk’s assistance providing notice of unauthorized access, and such assistance is not unduly burdensome to NoRedInk, NoRedInk shall notify the affected parent, legal guardian or eligible student of the unauthorized access, which shall include the information required in this Section 6.

Exhibit A
Additional State Covered Information Protection Laws

<i>Statute</i>	<i>As of Date</i>
Connecticut General Statutes 10-234aa – 10-234dd	2/21/2020
Illinois Student Online Personal Protection Act, 105 ILCS 85/1; Illinois School Student Records Act (ISSRA), 105 ILCS 10/1 et seq. & 23 IAC 375	2/21/2020
Montana Pupil Online Personal Information Protection Act (Montana House Bill 745)	2/21/2020
New York State Education Law Section 2-D	2/21/2020
Texas Education Code Chapter 32, Subchapter D	2/21/2020
Code of Virginia § 22.1-287.02	2/21/2020