

**Data Sharing and Confidentiality Agreement (Education Law 2-d Rider)**

**between the**

**ROCKY POINT UNION FREE SCHOOL DISTRICT**

**And**

**Kami Limited/Notable Inc.**

**8605 Santa Monica Blvd, PMB 57387, West Hollywood, CA 90069-4109**

*(Kami Limited/Notable Inc. provides Rocky Point students and staff resources related to document sharing, editing, and annotating.)*

Supplemental Agreement dated this 20<sup>th</sup> Day of October between the ROCKY POINT UNION FREE SCHOOL DISTRICT (the “District”), located at 90 ROCKY POINT-YAPHANK ROAD, ROCKY POINT, NEW YORK, 11778, and Kami Limited/Notable Inc.. (the “Contractor”) are parties to a contract or other written agreement pursuant to which Contractor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”) from the District for purposes of providing certain products or services to the District.

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

WHEREAS, the Vendor represents that it will only share Protected Information with third party subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of the Vendor under this Contract and all applicable New York State and Federal laws.

WHEREAS, the District and the Vendor wish to enter into an Agreement in order to comply with Education Law §2-d the Vendor agrees that it will comply with all terms set forth in the Agreement. To the extent that any terms contained in the Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that the Vendor has online or written Privacy Policies or Terms of Service (collectively, “TOS”) that would otherwise be applicable to its customers or users of the products or services that are the subject of the Agreement between the District and Contractor to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

NOW THEREFORE, in consideration of the mutual promises below, the District and the Vendor 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.
  - a. “Educational Agency” shall generally have the same meaning as the term Educational Agency at Education Law §2-d(1)(c), and in reference to the party to this Agreement

shall mean the ROCKY POINT UNION FREE SCHOOL DISTRICT.

- b. “Third Party Subcontractor” 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. “Protected Data” means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Agreement.
  - d. “Student” means any person attending or seeking to enroll in an Educational Agency.
  - e. “Student Data” means Personally Identifiable Information of a “Student.”
  - f. “Eligible Student” means a Student who is eighteen years or older.
  - g. “Parent” means a parent, legal guardian, or personal in parental relation to a Student.
  - h. “Building Principal” or “Principal” means a building principal subject to annual performance evaluation review under Education Law §3012-c.
  - i. “Classroom Teacher” or “Teacher” means a teacher subject to annual performance evaluation review under Education Law §3012-c.
  - j. “Teacher or Principal Data” means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Agreement..
  - k. “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 §3012c.
  - l. “NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).
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 the Vendor and are incorporated into this Supplemental Agreement. The Parents Bill of Rights for Data Privacy and Security states:
- a. A student's personally identifiable information cannot be sold or released for any commercial purposes.
  - b. Parents have the right to inspect and review the complete contents of their child's education record maintained by the Rocky Point Union Free School District.
  - c. State and federal laws protect the confidentiality of personally identifiable information. 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.

- d. A complete list of all student data elements collected by the State is available for public review at

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

or a copy may be obtained by writing to:

Office of Information & Reporting Services  
New York State Education Department, Room 863 EBA 89  
Washington Avenue  
Albany, NY 12234

- e. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

Aaron Factor, Executive Director of Curriculum, Technology, & Innovation  
Rocky Point UFSD  
90 Rocky Point-Yaphank Road  
Rocky Point, NY, 11778  
631-849-7080 [afactor@rockypoint.k12.ny.us](mailto:afactor@rockypoint.k12.ny.us)

- f. “Supplemental information” for each contract into which the District enters with a third party who receives student data or teacher or principal data shall:

- i. The exclusive purposes for which the student data or teacher or principal data will be used;
  - ii. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
  - iii. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
  - iv. 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; and
  - v. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
- g. This Bill of Rights 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), the District has developed the following “supplemental information” for the Agreement with the Vendor:

- a. Student Data and/or Teacher or Principal Data which the Vendor comes into possession as part of its Agreement with the District shall be used for the exclusive purpose(s) of performing Contractor’s obligations under this Agreement.
- b. The Vendor will ensure that any and all subcontractors, persons or entities that the Vendor may share the Student Data and/or Principal or Teacher Data with will abide by the terms of the Agreement, this Supplemental Agreement, 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 Vendor, the Vendor shall return such data to the District or if agreed to by the District, destroy the remaining Student Data and/or Principal or Teacher Data that the Vendor still maintains in any form in a manner agreeable to the district.
- 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 Vendor 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 Vendor hereby agree that the Student Data and/or Principal or Teacher Data shall be stored in the following manner:

In order to create a unique account, Kami does require that all users enter their email address and create a password, which is stored on the site, or use their own Google or Microsoft Account to sign on (Single-Sign-On), and may collect additional information such as name of school or class, and whether they are a teacher or student, in order to assign the user to the correct user group.

4. As required by Education Law §2-d(5)(e), the Vendor hereby agrees that any officers or employees of the Vendor, including any third-party 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.

People & Process • Within Kami, user data access is limited to staff who need this access to carry out their role, in order to provide the service to the user: customer support, engineering. • All Kami staff require SSH keys and 2FA-authentication (via hardware tokens) to access our secured networks. • Policies, training and processes are in place to ensure user data is not downloaded to staff local machines or storage devices and not printed to hardcopy. • Backup/archiving is carried out entirely within our partners’ secure data center network.

5. As required by Education Law §2-d(5)(f), the Vendor 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 Vendor 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 administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, and that align with the NIST Cybersecurity Framework 1.0;

- e. Store all data in the continental United States (CONUS) or Canada.
- f. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2).

6. Breach and unauthorized release of Personally Identifiable Information:

- a. In accordance with Education Law §2-d(6), the Vendor 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 Vendor 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 Vendor, 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. To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.
- d. In the case of notification to a Parent, Eligible Student, Teacher or Principal due to the unauthorized release of student data by the Vendor, or its subcontractors or assignees, the Vendor shall promptly reimburse the educational agency for the full cost of such notification, as required by Education Law §2-d(6)(c).

Outages, attacks, unauthorized use, or other factors may compromise the security of user information at any time. In the event of a security breach, we will notify you by posting on the Kami Website and notifying you by email using the email address on your account within 72 hours of Kami becoming aware of such breach.

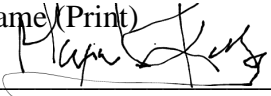
7. MISCELLANEOUS.

- 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 Vendor 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.

- d. This agreement expires June 30, 2024. Upon expiration of this Contract without a successor agreement in place, the Vendor shall assist the Rocky Point Union Free School District in exporting all Protected Information previously received from, or then owned by the Rocky Point Union Free School District.
- e. Upon expiration of this Contract with a successor agreement in place, the Vendor will cooperate with the Rocky Point Union Free School District as necessary to transition protected data to the successor vendor prior to deletion. The Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of the Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of the Vendor in secure data center facilities.
- f. The Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by the Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

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

BY THE VENDOR: Kami Limited/Notable Inc.

\_\_\_\_\_  
Maxine R. Kalnitz  
Name (Print)  
  
\_\_\_\_\_  
Signature  
\_\_\_\_\_  
Northeast Account Executive  
\_\_\_\_\_  
Title  
\_\_\_\_\_  
10/20/2021  
\_\_\_\_\_  
Date

# Security and Data Protection Measures

Kami

December, 2019

THIS DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

The information in this document is confidential and meant for use only by the intended recipient and only in connection with and subject to the terms of its contractual relationship with Kami. Acceptance and/or use of any of the information contained in this document indicates agreement not to disclose or otherwise make available to any person who is not an employee of the intended recipient, or to any other entity, any of the information contained herein. This documentation has the sole purpose of providing information regarding a Kami software product or service and shall be disclosed only to those individuals who have a need to know.

Any entity or person with access to this information shall be subject to this confidentiality statement.

No part of this publication may be reproduced or transmitted in any form or by any means for any purpose without the express written permission of Kami.

Copyright © 2017, 2018, 2019 Kami Limited. All rights reserved.  
Kami is a trademark of Kami Limited.  
214 Karangahape Road, 1st floor, Auckland 1010, New Zealand



To protect the security and privacy of your data, Kami employs a well-designed infrastructure and adheres to industry best practices.

## System Architecture

### Data encryption

- Encryption is used during transit for connections between users' browsers and our backend services. We employ industry best-standard cipher suites and protocols - currently TLS 1.2 with ECDHE\_RSA key exchange and AES encryption.
- We use HSTS to ensure all HTTP requests through our domains shall always be encrypted and prevent MITM attacks.
- Data is protected at rest using encryption provided by our cloud services providers (Amazon Web Services and Google Cloud Platform).
- Kami is exposed to the same level of vulnerability of the AWS and Google Cloud platforms as other users of any technology stack; we ensure all latest security patches are promptly applied relating to our full technology stack.

### Network protection

- We employ Google's "Beyondcorp" approach to enterprise security of zero-trust networks. Applications on said isolated networks employ best practices to ensure that they'd be considered secure even if they were accessible from the open web.
- Firewalls are used to segregate application tiers and provide strict controls on access to resources within our networks. Our services are also separated into separate networks using Amazon's Virtual Private Cloud technology and Google's Cloud Networking to provide an additional layer of protection.

### Disaster recovery and backups

- Your data is protected using streaming replication to geographically distributed backup servers and log shipping to secure storage. We create daily backups using multiple independent systems and store them across multiple different providers. Our backups are encrypted on dm-crypt encrypted disks with strong passwords.
- We conduct disaster recovery drills quarterly to ensure we can quickly restore services without data loss in cases of emergency.

## Secure networks and data centers

Staff require SSH keys and 2FA-login (via hardware tokens) to access our networks.

We implement best-practice protective measures against attacks including XSS, CSRF, and SQL injection.

Amazon Web Services (AWS) and Google Cloud Platform (GCP) power the server requirements for thousands of high-profile companies and government entities. We have chosen these providers because of their stringent security measures, which include compliance with the following certifications and third-party attestations:

- SAS70 Type II audits
- Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS)
- ISO 27001 certification
- U.S. General Services Administration FISMA-Moderate level operation authorization

Read more about the security provided by [AWS](#) and [Google Cloud Platform](#).

## Password authentication

- We support both authentication with a username and password, and SSO through Google OAuth.
- Passwords are stored using bcrypt with a high stretching factor.

## Data Stored

- Kami stores data in the secure data centers operated by our cloud hosting partners Amazon Web Services (AWS) and Google Cloud Platform (GCP).

- Kami only collects data that is used explicitly required to provide and maintain the service to you

Category	Elements
Application technology meta data	IP address, cookies
Application usage statistics	meta data on interaction with application
Authentication	Oauth key
User information	First name, last name (if entered by user), email address
User-generated data	<p>Filenames, annotations, comments.</p> <p>A Document itself is only uploaded to Kami servers if shared by the user with other users for collaborative annotation. These uploaded Documents are fingerprinted and shared only, and are not stored persistently on Kami servers. (The sharing function may optionally be disabled for a given domain)</p>

## People & Process

- Within Kami, user data access is limited to staff who need this access to carry out their role, in order to provide the service to the user: customer support, engineering.
- All Kami staff require SSH keys and 2FA-authentication (via hardware tokens) to access our secured networks.
- Policies, training and processes are in place to ensure user data is not downloaded to staff local machines or storage devices and not printed to hardcopy.
- Backup/archiving is carried out entirely within our partners' secure data center network.

## Content Ownership and Data Privacy

- Kami claims no ownership over any content - information, documents or data - created or stored using our services. You retain copyright and any other rights, including all intellectual property rights, on created content and included content.
- Your content is only accessible to other Kami users you explicitly shared it with.
- We respect your privacy and will never share your content or personal data or make your content publicly available without your permission.
- Refer to our [standard terms and conditions](#), and our [privacy policy](#) for further details.

