RCSD ROSEVILLE CITY SCHOOL DISTRICT
Est. 1869

Technology Services

1050 Main Street Roseville, CA 95678
Phone (916) 771-1645 Fax (916) 771-1650

Laura Assem, Director of Technology

Vendor Statement of Compliance
Data Privacy and Protection

This agreement is entered into between the Roseville City School District ("LEA" or "District") and Notable Inc (dba Kami) ("Service Provider") on 11/25/2019 ("Effective Date").

WHEREAS, the LEA and the Service Provider entered into an agreement for Educational Technology services;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015, between a local education agency and a third-party service provider must include certain terms;

NOW, THEREFORE, the Parties agree as follows:

Section I: General - All Data

1. **PASSWORD SECURITY.** All passwords are considered secure. Vendors may not disseminate any passwords unless specifically directed by Educational or Technology Services management. Vendors will not provide information concerning Admin accounts (ROOT Admin, container Admin, local NT administrator or Domain administrator) or their equivalent to any persons. District personnel ONLY will disseminate this information. Vendors will never create "back door" or "generic" user accounts on any systems unless specifically directed to do so by LEA management.

   Agree: Yes ● No ○

2. **SYSTEM SECURITY.** Unauthorized access to or modification of District systems including file servers, routers, switches, NDS and Internet services is prohibited. Any attempt to bypass or subvert any District security system, both hardware, and software is prohibited.

   Agree: Yes ● No ○

3. **PRIVACY**. The vendor will adhere to all provisions of the Federal Family Educational Rights and Privacy Act (FERPA, 20 U.S.C. 123g), California Education Code and district policies regarding the protection and confidentiality of data. At all times, the vendor will consider all data collected in the course of their duties to be protected and confidential. Release of this data can only be authorized by Technology & Information Services management and state and federal law.

   Agree: Yes ● No ○

Section I: General - All Data *(Continued)*

4. **REUSE**: Vendors shall not copy, duplicate, sell, repackage or use for demonstration purposes any Roseville City School District data without the prior, written consent of Educational or Technology Services management.

   Agree: Yes ● No ○

5. **TRANSPORT**: Vendor must provide a secure channel (S/FTP, HTTPS, SSH, VPN, etc) for the District to "push" data to the vendor and to extract data as required. Vendors will not have direct access to District systems and will not "pull" data at any time.

   Agree: Yes ● No ○

6. **EXTERNAL SECURITY:** Vendor must attach to this document reasonable evidence that their system is secure from external hacking and attacks. Devices such as firewalls and technologies such as NAT are the minimum requirements. Active IDS or similar technology is preferred.

   Agree: Yes ● No ○

7. **INTERNAL SECURITY:** Vendors must attach to this document reasonable evidence that their system is secure from internal hacking and attacks. Describe the interactions vendor personal (or their representatives) will have directly with District data. How is uploaded data from the District handled and processed? Who has access to this data? What happens to the data after the upload is complete? What security safeguards are in place to protected unauthorized access to District data? How are backup performed and who has access to and custody of the backup media? How long are backup maintained; what happens to the District data once the backup is "expired"? If any data is printed, what happens to these hard copy records?

   Agree: Yes ● No ○

8. **DISTRICT ACCESS:** Vendor must provide a secure means (see Item 5 above) for the District to extract ALL data from the vendor system. This can either be an online extraction tool or a vendor-provided extract as needed by the District (not to exceed quarterly). Describe the means and format of the data (delimited, Excel, MDB, SQL Dump).

   Agree: Yes ● No ○ *Student documents are not stored on Kami servers, but on their own storage*

9. **TERMINATION:** Upon termination of this agreement as provided herein, the vendor will permanently delete all customer data from their system as allowed by state and federal law. Vendor may be required to certify the destruction of LEA data within 90 days of contract termination.

   Agree: Yes ● No ○

Section II: AB1584 Compliance - Student Information Only

1. Vendor agrees that the Roseville City School District retains ownership and control of all student data.

   Agree: Yes ● No ○

2. Vendor must attach to this document a description of how student-created content can be exported and/or transferred to a personal account.

   Agree: Yes ● No ○ *Not necessary: All student content is saved to their own storage (Google Drive or local device)*

3. Vendor is prohibited from allowing third-parties access to student information beyond those purposes defined in the contract.

   Agree: Yes ● No ○

4. Vendor must attach to this document a description of how parents, legal guardians and students can review and correct their personally identifiable information.

   Agree: Yes ● No ○

5. Vendor will attach to this document evidence how student data is kept secure and confidential.

   Agree: Yes ● No ○

6. Vendor will attach to this document a description of procedures for notifying affected parents, legal guardians or eligible students when there is an unauthorized disclosure of student records.

   Agree: Yes ● No ○

7. Vendor certifies that student records will not be retained or available to a third party once the contract has expired or is canceled (See Page 2, Item 9).

   Agree: Yes ● No ○

8. Vendor will attach to this document a description of how they and any third party affiliates comply with FERPA.

   Agree: Yes ● No ○

9. Vendor and its agents or third parties are prohibited from using personally identifiable information from student records to target advertising to students

   Agree: Yes ● No ○

Section III: SB 1177 SOPIPA Compliance - Student Information Only

1. Vendors cannot target advertising on their website or any other website using information acquired from students.

   Agree: Yes ● No ○

2. Vendors cannot create a profile for a student except for school purposes as defined in the executed contract.

   Agree: Yes ● No ○

3. Vendors cannot sell student information.

   Agree: Yes ● No ○

4. Vendors cannot disclose student information unless for legal, regulatory, judicial, safety or operational improvement reasons.

   Agree: Yes ● No ○

5. Vendors must attach to this document evidence of how student information is protected through reasonable security procedures and practices.

   Agree: Yes ● No ○

6. Vendors must delete district-controlled student information when requested by the District.

   Agree: Yes ● No ○

7. Vendors must disclose student information when required by law, for legitimate research purposes and for school purposes to educational agencies.

   Agree: Yes ● No ○

As an authorized representative of my organization, I accept the conditions listed in this document.

Bob Drummond
Print Name

12/2/2019
Signature, Date

Laura Assem, 12/2/2019
Print Name (Roseville City School District)

Laura Assem
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Refer to attached "Kami Data Security measures July2019.PDF"

Section 1.7: Internal Security

Refer to attached "Kami Data Security measures July2019.PDF"

Section II.2: Exporting of Student-Created Content

Student content is saved in their own Google Drive or can be downloaded to their local machine. Documents are not stored on Kami servers.

Section II.4: Review and Correcting Personally Identifiable Information (PII)

Refer to process outlined in Kami Student Data Privacy Policy at https://www.kamiapp.com/coppa-privacy-policy-2/
"If youwish to review your or your student's or your child's personally identifiable information stored by Kami, you mayemail usyour request atprivacy@kamiapp.com. We will respond to your request within 30 days. If your or your student's or your child's personally identifiable information changes, or if you no longer desire our service, you may correct, update, or delete it by making the change directly in the user profile in the Kami App, or email us atprivacy@kamiapp.com. We will respond to your request within 30 days."

EXHIBITS

Section II.5: Securing Student Data

Refer to attached "Kami Data Security measures July2019.PDF"

Section II.6: Disclosure Notification

Refer to "Disclosure and Permissions" section in Kami Student Data Privacy Policy at https://www.kamiapp.com/coppa-privacy-policy-2/ :
We do not disclose personal information collected from Children to third parties other than to persons who provide support for the operations of the service and who do not use the information for any other purpose, except Parents, Teachers & school administrators. If required by Law to disclose user data, we will notify the school.

Section II.8: Family Educational Rights and Privacy Act (FERPA) Compliance

Refer to processes outlined in Kami Student Data Privacy Policy at https://www.kamiapp.com/coppa-privacy-policy-2/

Section III.5: How Student Data is Protected:

Refer to attached "Kami Data Security measures July2019.PDF"

Reset Form

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.

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	Filenames, annotations, comments. 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)

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.