



PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Health Sciences Charter School (HSCS) 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, Health Sciences Charter School informs the school community of the following:

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 education record.
3. State and federal laws protect the confidentiality of personally identifiable 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 public review at the following website <http://www.nysed.gov/data-privacy-security/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
5. Parents have the right to submit complaints about possible breaches of student data addressed. Complaints may be directed in writing to Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234 or by using the form available at the following website: <http://www.nysed.gov/data-privacy-security/report-improper-disclosure>

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the day and year first written above.

A handwritten signature in black ink, appearing to be a stylized name, written over a horizontal line.

Authorized Vendor Signature

Date

A handwritten signature in black ink that reads "EREN REYNOLDS", written over a horizontal line.

Authorized HSCS Signature

Date



VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY

Vendor:		Product:	
Collects:	Student Data	Teacher or Principal Data	Does Not Collect Either

Educational agencies including Health Sciences Charter School are required to post information about [third-party contracts](#) on the agency's website with the Parents Bill of Rights. To that end, please complete the table below with information relevant to [NYS Education Law 2-d](#) and [Part 121.3 of the Commissioner's Regulations](#). Note that this applies to all software applications and to mobile applications ("apps").

PART 1: Exclusive Purpose for Data Use
The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor:
PART 2: Subcontractor Oversight Details – Select the appropriate option below
This Contractor has no subcontractors
This contract has subcontractors. As such, the third-party contractor will take the following steps to ensure that any subcontractors, assignees, or other agents who see, or receive, this protected data are contractually required to obey the same data protection and security requirements that the third-party contractor is required to obey under state and federal law: contract terms
PART 3: Contract Lifecycle Practices
The contract expires on _____ unless renewed or automatically extended for a term pursuant to the agreement. When the contract expires, protected data will be deleted by the contractor, via shredding, returning of data, mass deletion, and upon request, may be exported for use by HSCS before deletion.
Part 4: Student Educational Records / Improper Disclosure
A. For information on FERPA (Family Educational Rights and Privacy Act), which is the federal law that protects the privacy of student education records, visit the U.S. Department of Education FERPA website .
B. A complaint or report of improper disclosure may be completed by submitting the Improper Disclosure Report form .
Part 5: Security Practices
A. Protected data provided to the contractor will be stored: (include where and how)
B. The security protections taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry best practices include:
Part 6: Encryption Practices
By checking this box, contractor certifies that data encryption is applied in accordance with NYS Education Law Section 2-d 5(f)(5) .

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.

