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, Executive 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 Happy Numbers Inc. ("Service Provider") on 09/18/2023 ("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 ○

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 ○

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.

Evgeny Milyutin
Print Name

DocuSigned by:
0B1C4983C00645C...
9/18/2023
Signature, Date

Laura Assem
Print Name (Roseville City School District)

09/18/2023
Signature, Date (Roseville City School District)

EXHIBITS

Section 1.6: External Security

Happy Numbers Inc. will 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. Happy Numbers Inc. will use encryption technology to protect data in motion or 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).

Section 1.7: Internal Security

Minimizing the Use, Collection, and Retention of PII: We only store the minimum information required for the proper functioning of our application. This includes students' first and last names (no students' emails, addresses, etc.), group names, and the names and emails of teachers, as well as the school name. This constitutes nearly all the data we store. We collect minimal information from single sign-on (SSO) systems such as ClassLink and Clever.

Anonymizing Information: We have a special tool to prepare databases for test and development environments with complete anonymization of PII. Developers and QA engineers cannot access real personal data throughout the development lifecycle.

Access Enforcement: All employees have their personal auditable accounts in all our systems. We use Single Sign-On to grant access to all internal systems. The critical applications, such as the admin panel, have RBAC for different access levels.

Separation of Duties: We adhere to the principle of minimizing access, which means that, for instance, a content manager can access the BI system with de-identified student problem-solving logs, but they do not have access to the admin panel with actual data.

Least Privilege: Our internal systems use an RBAC model to grant each employee the minimum required access level.

Remote Access: All types of communication with our servers and systems are encrypted using battle-tested protocols, such as enforced HTTPS with TLS 1.2, SSH, and OpenVPN.

Auditable Events: We collect all change events in our SSO system and admin panel and store them in a database without making any modifications.

Protection of Information at Rest: We store our backups in AWS S3 using the pgBackRest tool with AES-256-CBC encryption. Furthermore, our application servers transparently encrypt sensitive personal information, such as students' first and last names, using a symmetric cipher before storing it in an encrypted database.

Data Backup and Recovery: We continuously back up all production PostgreSQL databases using the pgBackRest tool and retain data for 30 days, including four weekly full backups.

Change Management: Our infrastructure is entirely managed by Infrastructure as Code (IaaC) tools, including a custom in-house CLI tool, Terraform, and Ansible. This means that all changes can be reviewed through standard development procedures and are stored in GitHub.

Section II.2: Exporting of Student-Created Content

N/A
Students do not create any content while using HappyNumbers.com

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

Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the LEA. If a correction to data is deemed necessary, the LEA will notify Happy Numbers Inc. We agree to facilitate such corrections within 21 days of receiving the LEA’ s written request.

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, Executive Director of Technology

EXHIBITS

Section II.5: Securing Student Data

Happy Numbers Inc. will implement all state, federal, and local data security and privacy requirements, consistent with the School District's Data Security and Privacy Policy in the following way(s): Happy Numbers Inc. complies with the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA).
For more information, please, see:
Privacy Policy: https://happynumbers.com/privacy-policy
Terms of Service: https://happynumbers.com/terms-of-service

Section II.6: Disclosure Notification

In the event, that we become aware of an unauthorized disclosure or data breach:
- the District and teachers will be notified by email if the teacher account or any related student accounts are affected within 24 hours.
- the appropriate person in the school or district who purchased the valid school-wide or district-wide Happy Numbers access will be notified by phone if the users from this school or district are affected within 24 hours.

The notice must contain the following information:
- data of the breach;
- the types of information that were subject to the breach;
- general description of what occurred;
- steps we are taking to address the breach;
- the contact person at Happy Numbers whom the data holder can contact.

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

Parents and eligible students are granted following rights under FERPA and Happy Numbers' Terms of Service and Privacy Policy:
- the right to inspect and review their records,
- the right to request that their records be corrected,
- the right to file a complaint.

Minors are only allowed to use our Website with their legal representative’ s consent.
Happy Numbers has been granted the iKeepSafe California Student Privacy Badge, which validates our compliance with FERPA.

Section III.5: How Student Data is Protected:

All the data is stored in isolated VPC Google Cloud servers located in the US. All sensitive data is stored in encrypted using an ansible-vault mechanism on Google Cloud servers. In addition, we use TLS v1.2 to transit data. To safeguard the data we keep, we use a restricted network, and to access it, we use a regularly updated VPN with encryption.