DATA SHARING AND CONFIDENTIALITY AGREEMENT

INCLUDING

Bill of Rights for Data Privacy and Security

AND

Vendor Information Regarding Data Privacy and Security

This Data Sharing and Confidentiality Agreement (the "Agreement") is made and entered into by and between Happy Numbers Inc. (the "Vendor") and **Cuba-Rushford Central School** ("CRCS").

WHEREAS, CRCS and Vendor are parties to a contract or other written agreement (the "Contract") pursuant to which the Vendor will receive student data and/or teacher or principal data ("Protected 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 CRCS for purposes of providing certain products or services to CRCS; and

WHEREAS, both CRCS and Vendor are desirous of fulfilling their respective obligations under New York Education Law Section 2-d;

NOW THEREFORE, in consideration of the mutual promises and covenants contained in the Contract, as well as, this Agreement the parties hereto mutually agree as follows:

1. **Confidentiality**

   a. Vendor, its employees, and/or agents agree that all information obtained in connection with the services provided for in the Agreement is deemed confidential information.

   b. Vendor further agrees to maintain the confidentiality of the Protected Data it receives in accordance with federal and state law and that any information obtained will not be revealed to any persons, firms or organizations.

2. **Data Protections and Internal Controls**

   a. Vendor acknowledges that it may receive and/or come into contact with personally identifiable information, as defined by New York Education Law Section 2-d, from records maintained by CRCS that directly relate to a student(s) (hereinafter referred to as "education record").

   b. Vendor understands and acknowledges that it shall have in place sufficient protections and internal controls to ensure that information is safeguarded in accordance with applicable laws and regulations, and understands and agrees that it is responsible for complying with state data security and privacy standards for all personally identifiable information from education records, and it shall:

      1. Limit internal access to education records to those individuals that are determined to have legitimate educational interests; and

      2. Not use the education records for any other purpose than those explicitly authorized in the Contract and/or Agreement; and

3. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of education records in its custody; and

4. To use encryption technology to protect Protected Data in its custody while in motion or at rest, using a technology or methodology specified by the secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

3. <u>Data Security and Privacy Plan</u>

a. Vendor agrees to have a Data Security and Privacy Plan in place to protect the confidentiality, privacy and security of the Protected Data it receives from CRCS.

b. Vendor understands and agrees that it is responsible for submitting a Data Security and Privacy Plan to CRCS prior to the start of the term of the Agreement, and it shall:

1. Outline how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract consistent with CRCS's policy on data security and privacy, as adopted.

2. Outline specific administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from CRCS under the Contract.

3. Outline the training requirement established by the Vendor for all employees who will receive personally identifiable information from student records (hereinafter referred to as "student data").

4. <u>Notice of Breach and Unauthorized Release</u>

a. In the event of a breach of this Agreement and unauthorized release of student data, the Vendor shall:

1. Immediately notify CRCS in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Vendor has discovered or been informed of the breach or authorized release.

2. Advise CRCS as to the nature of the breach and steps Vendor has taken to minimize said breach.

b. In the case of required notification to a parent or eligible student, the Vendor shall:

1. Promptly reimburse CRCS for the full costs of such notification.

c. Vendor will cooperate with CRCS and provide as much information as possible directly to CRCS about the incident, including but not limited to:

1. The description of the incident;

2. The date of the incident;

3. The date Vendor discovered or was informed of the incident;

4. A description of the types of Protected Data involved;

5. An estimate of the number of records affected;

6. The schools within CRCS affected;

7. What the Vendor has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data; and

8. The contact information for Vendor representatives who can assist affected individuals that may have additional questions.

d. The Vendor shall indemnify and hold CRCS harmless from any claims arising from its breach within the Data Sharing and Confidentiality Agreement confidentiality and data security and privacy standards provision.

e. Vendor acknowledges that upon initial notification from Vendor, CRCS, as the educational agency with which Vendor contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Vendor agrees not to provide this notification to the CPO directly unless requested by CRCS or otherwise required by law. In the event the CPO contacts Vendor directly or requests more information from Vendor regarding the incident after having been initially informed of the incident by CRCS, Vendor will promptly inform CRCS of the same.

5. <u>Vendor Information</u>

Vendor understands that as part of CRCS's obligations under New York Education Law Section 2-d, Vendor is responsible for providing CRCS with Vendor information (see Vendor Information for Data Privacy and Security) to include:

a. Exclusive purposes for which the student data will be used;

b. How Vendor will ensure that subcontractors, persons or entities that Vendor will share the student data with, if any, will abide by data protection and security requirements;

c. Vendor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student;

d. Vendor will not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

e. Vendor will provide a description of what will happen to the personally identifiable information upon expiration of the written agreement (e.g. whether, when and in what format the personally identifiable information will be returned to the educational agency, and/or whether, when and how the personally identifiable information will be destroyed).

f. If and how a parent, student, or eligible teacher may challenge the accuracy of the student/teacher data that is collected; and

g. Where the student 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.

6. <u>Termination or Expiration of Contract and/or Agreement</u>

a. Upon termination of the Agreement, Vendor shall return or destroy all confidential information obtained in connection with the services provided therein and/or student data. Destruction of the confidential information and/or student data shall be accomplished utilizing an approved method of confidential destruction, including, shredding, burning or certified/witnessed destruction of physical materials and verified erasure of magnetic media using approved methods of electronic file destruction. The parties further agree that the terms and conditions set forth herein shall survive the expiration and/or termination of the Agreement.

b. If requested by CRCS, Vendor will assist CRCS in exporting all Protected Data previously received back to CRCS for its own use, prior to deletion, in such formats as may be requested by CRCS.

c. In the event the Contract is assigned to a successor Vendor (to the extent authorized by the Contract), the Vendor will cooperate with CRCS as necessary to transition Protected Data to the successor Vendor prior to deletion.

d. Neither Vendor nor any of its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data will retain any Protected Data, copies, summaries or extracts of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Vendor and/or its subcontractors or other authorized persons or entities to whom it has disclosed Protected Data, as applicable, will provide CRCS with a certification from an appropriate officer that these requirements have been satisfied in full.

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

CRCS 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, CRCS 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 should be directed in writing to CRCS Data Privacy Officer, 5476 Route 305, Cuba, New York 14727. Complaints may also 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.

DocuSigned by:
Eugeny Milyutin
0B1C4983C00645C...

Authorized Vendor Signature

7/9/2021
Date

Authorized CRCS Signature

7/9/2021
Date

VENDOR INFORMATION REGARDING DATA PRIVACY AND SECURITY

Vendor: Happy Numbers Inc. Product: HappyNumbers.com

Collects: ☑ Student Data ☑ Teacher or Principal Data ☐ Does not collect either

Educational agencies including Cattaraugus-Allegany-Erie-Wyoming BOCES 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 Purposes for Data Use	**RESPONSE REQUIRED**
The exclusive purposes for which the student data (or teacher or principal data) will be used by the third-party contractor: The data is used to provide the functionality of the services. For more information, please, see the Privacy Policy: https://happynumbers.com/privacy-policy.	
Part 2: Subcontractor Oversight Details	**RESPONSE REQUIRED**
☐ This contract 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: Happy Numbers Inc. reviews the subcontractors' terms of service, privacy policy, and signs additional agreements with the subcontractors if needed.	
Part 3: Contract Lifecycle Practices	**RESPONSE REQUIRED**
The contract expires on on June 30th 2022 unless renewed or automatically extended for a term pursuant to the agreement. When the contract expires, the following will happen to the personally identifiable information (e.g. whether, when and in what format the personally identifiable information will be returned to the educational agency, and/or whether, when and how the personally identifiable information will be destroyed): Happy Numbers Inc. supports the secure deletion of the data.	
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	**RESPONSE REQUIRED**
A. Protected data provided to the contractor will be stored: (include *where* and *how*) All sensitive data is stored in encrypted using an ansible-vault mechanism on Google Cloud servers. B. The security protections taken to ensure data will be protected that align with the NIST Cybersecurity Framework and industry best practices include: Happy Numbers Inc. uses 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. We also have the following administrative, operational, and technical safeguards and practices to protect personally identifiable information listed in Appendix A.	
Part 6: Encryption Practices	**RESPONSE REQUIRED**
☑ By checking this box, contractor certifies that data encryption is applied in accordance with NYS Education Law Section 2-d 5(f)(5).	

Appendix A

Security Audit Checklist for Happy Numbers Inc.

This checklist describes the regular security audit processes for Happy Numbers Inc. It includes the checklist for the assets (physical and informational), list of threats and preventive & protective measures against these threats (action list).

This audit must be done at least twice a year. Also the appropriate measures should take place in case the new employee joins/leaves the company.

Assets List

- Laptops, Phones, Tablets (work and personal)
- Production environment VPN keys
- SSH Keys
- Backups
- Source codes (github)
- Stage environments
- Logs
- Email
- Production admin accounts
- Production tokens

Checklist / Action List

Common procedures:

- Store and keep in fit a list of employees who have any access to sensitive or/and personal information.

Devices hacking (viruses, trojans and so on)

- Regular check and educate each employee with simple rules of security:
    - 2Factor auth for all critical apps (especially gmail.com and github.com)
    - Encrypt disks of all laptops
    - Strong passwords (8 and more letters, digits, special symbols) on all laptops account and services
    - Password and/or fingerprint protection of all phones/tablets with the access to any work data including email

    - No pass for any sensitive information through open channels (emails, messaging apps, chats and so on). Use PGP or special password managers (like LastPass)

Illegal admin panel access

- Keep in fit list of superuser accounts on production and staging environments
- Remove superuser account after employee firing
- Allow to set strong passwords only for superusers
- Force HTTPS using for all applications including app to app communication

General Application Security

- Check all security bulletins for used soft (at the least NGINX, OpenVPN, Ruby on Rails, Postgresql, iptables and other) and apply security patches accordingly
- Regular apply OS security updates on all servers
- Keep each application in isolated private network with own VPN access
- Staging and testing environments are located in separated private network and use only anonymized databases or filled with fake data
- In all production environment close all ports (except, openvpn, http, https) with iptables
- Be sure all backups are stored encrypted on S3

Unauthorized private network access

- Repeatedly update all VPN keys and revoke old ones

Intentional (or unintentional) data/code damage

- Daily backups on S3 with write only access

3rdParty Tokens compromise

- Regularly verify:
    a) No use of production tokens in staging and dev environment
    b) All sensitive data is stored in encrypted using ansible-vault mechanism