CAYUGA ONONDAGA BOCES

DATA PRIVACY AGREEMENT

This Data Privacy Agreement ("DPA") is by and between the Cayuga Onondaga BOCES (the "BOCES") and Happy Numbers Inc. (the "Contractor"), collectively referred to as the "Parties.".

Section 1: Definitions

1. **"Breach"** means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.
2. **"Commercial Purpose" or "Marketing Purpose"** means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve or market products or services to students.
3. **"Disclose" or "Disclosure"** means to permit access to, or the release, transfer, or other communication of Personally Identifiable Information (as defined below) by any means, including oral, written, or electronic, whether intended or unintended.
4. **"Education Records"** means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **"Eligible Student"** means a student who is eighteen years or older.
6. **"Encryption"** means methods of rendering Personally Identifiable Information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted 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.
7. **"Parent"** means a parent, legal guardian, or person in parental relation to a student.
8. **"Personally Identifiable Information,"** as applied to student data, means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and as applied to teacher and principal data, means personally identifiable information as such term is defined in N.Y. Education Law §3012-c (10).
9. **"Release"** shall have the same meaning as Disclosure or Disclose.
10. **"Student"** means any person attending or seeking to enroll in an educational agency.
11. **"Student data"** means Personally Identifiable Information from the student records of an educational agency. For purposes of this Schedule B, "student data" includes information made accessible to Contractor by BOCES, BOCES officers, BOCES employees, BOCES agents, BOCES students, and/or the officers, employees, agents, and/or students of educational agencies with whom BOCES contracts.
12. **"Teacher or principal data"** means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of N.Y. Education Law §§ 3012-c and 3012-d. For purposes of this Schedule, "student data" includes information made accessible to Contractor by BOCES, BOCES officers, BOCES employees, BOCES agents, BOCES students, and/or the officers, employees, agents, and/or students of educational agencies that contract with BOCES in order to access Contractor's services.
13. **"Unauthorized Disclosure" or "Unauthorized Release"** means any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

Section 2: Data Privacy

1. **Compliance with Law:** The Contractor's storage, use and transmission of student and teacher/principal PII shall be consistent with this DPA and applicable state and federal laws and regulations that protect the confidentiality of PII.
2. **Authorized Use:** The Contractor shall not sell PII nor use or disclose it for any marketing or commercial purpose or permit another party to do so. The Contractor shall not use PII for any purpose other than the provision of the services described in this DPA only for the term of the engagement of said services.
3. **Data Security/Encryption:** The Contractor shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which will align with the NIST Cybersecurity Framework, including:
   a. PII data will be protected using encryption while in motion and at rest by hard drive encryption, TLS. AES-256, and HTTPS web encryption depending on the secure system used to transport or store the data.
   b. PII will be stored in a manner as to protect its security and to mitigate any security risks. Specifically, all student data and/or teacher or principal data will be stored by saving it to our document management system (highly secure with all activity logged). The security of this data will be ensured by encryption and user access control.
   c. Physical access to PII by individuals or entities described in paragraph 3 above shall be controlled as follows: All access to sensitive data will be controlled by and limited to the team working on the contract subject matter and all access will be ensured by encryption and user access control.
4. **Employees and Subcontractors:** The Contractor shall ensure that PII is not disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Contract. The Contractor agrees that it will not utilize any subcontractors or outside entities to provide services under the Contract and shall not disclose any PII other than as required in this DPA. Contractor shall ensure that all employees and subcontractors comply with the terms of this DPA and are provided with any training on all applicable state and federal laws and regulations that protect the confidentiality of PII before being provided access to PII. If disclosure of PII is required by law or court order, the Contractor shall notify the BOCES and New York State Education Department no later than the time the PII disclosure is required unless such notice is expressly prohibited by law or the court order.
5. **Data Return/Destruction:** Upon expiration of the contract, all PII will be returned to the BOCES in a manner and format agreed upon by the Parties, and/or destroyed and purged from the Contractor's systems in a manner that does not allow it to be retrieved or read. Contractor acknowledges it is prohibited from retaining PII Or having continued access to PII beyond the term of this DPA.
6. **Parent/Eligible Student Access:** Parents and Eligible Students have the right to inspect and review their or their child's PII stored or maintained by the contractor. Contractor shall respond within thirty (30) calendar days to the BOCES requests for access to Student Data so the BOCES can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held

by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the BOCES and refer the Parent or Eligible Student to the BOCES.

7. **Breach:** The Contractor shall take the following steps to identify breaches or unauthorized releases of PII and notify the BOCES upon learning of an unauthorized release of PII:
   a. Provide prompt notification to the BOCES no later than seven (7) calendar days from the date of discovery of a breach or unauthorized release of PII. The Contractor shall provide notification to the BOCES' Data Privacy Officer, by phone at (315) 255-7670 and by email at dataprivacyofficer@cayboces.org
   b. The Contractor shall cooperate with the BOCES and law enforcement to protect the integrity of any investigation of any breach or unauthorized release of PII.
   c. Where a breach or unauthorized release is attributed to the Contractor, the Contractor shall pay for or promptly reimburse the BOCES for the full cost of the notification.
8. **Termination:** The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.
9. **Bill of Rights for Data Privacy and Security**: As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the BOCES is required to post the completed Exhibit B on its website.
10. 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 parents may obtain a copy of this list by writing to the Office of Information and Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
11. Parents have the right to file complaints with the BOCES about possible privacy breaches of student data by the BOCES' third-party contractors or their employees, officers, or assignees, or with the NYSED. Complaints to the NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, email to CPO@mail.nysed.gov.

DocuSigned by:
0B1C4983C00645C...

Contractor Signature

Evgeny Milyutin

Printed Name

CEO

Title

1/19/2024

Date

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the BOCES' Data Privacy Officer by email at dataprivacyofficer@cayboces.org (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

EXHIBIT B

Supplemental Information to Parents Bill or Rights for Data Privacy and Security

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the BOCES is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Happy Numbers Inc.
Name(s) of Covered Applications	HappyNumbers.com
Type of PII that Contractor will receive/access	Student PII: ☑ Collected □ Not Collected APPR Data: ☑ Collected □ Not Collected
Contract Term	Contract Start Date 1/1/2024 Contract End Date 6/30/2026
Subcontractor Written Agreement Requirement	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) □ Contractor will not utilize subcontractors. ☑ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to BOCES, or a successor contractor at the BOCES option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.

Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the BOCES. If a correction to data is deemed necessary, the BOCES will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the BOCES' written request.
Secure Storage and Data Security	Any Protected Data Vendor receives will be stored on systems maintained by Vendor, or by a subcontractor under the direct control of Vendor, in a secure data center facility located within the United States. The measures that Vendor will take to protect Protected Data include adoption of technologies, safeguards and practices that align with the NIST Cybersecurity Framework and industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
Encryption	Data will be encrypted while in motion and at rest.

DATA SECURITY AND PRIVACY PLAN

Under the requirements under 8 NYCRR 121, Happy Numbers Inc. maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

1. 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), New York Education Law §3012-c, and New York State Education Law §2-d.

Privacy Policy: https://happynumbers.com/privacy-policy
Terms of Service: https://happynumbers.com/terms-of-service

2. Happy Numbers Inc. has in place the following administrative, operational, and technical safeguards and practices to protect personally identifiable information listed in Appendix A.

3. Happy Numbers Inc. shall comply with 8 NYCRR 121 in that it acknowledges that it has reviewed the School District’s Parents Bill of Rights for Data Privacy and Security and will abide by it.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Happy Numbers Inc. and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing the confidentiality of such data. Each employee shall receive such training on April 1 of each calendar year. Officer(s) and employee(s) of Happy Numbers Inc. who have completed data privacy and protection training are granted certificates of completion after passing a quiz or assessment related to the training material.

5. Happy Numbers Inc. shall utilize subcontractors and manage the relationships and contracts with such subcontractors in a way that ensures that subcontractors comply with data protection regulations and standards, including but not limited to FERPA, New York Education Law §3012-c, New York State Education Law §2-d. This includes reviewing the existing terms of service the privacy policy of the subcontractor, and signing additional agreements and NDAs with the subcontractor if needed. Happy Numbers Inc. maintains a third-party risk management program to ensure that such

subcontractors abide by applicable data protection and security requirements of this Plan and agreement with the District.

6. 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).

Administrative and Operational Safeguards:

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.

7. Happy Numbers Inc. has the following procedures, plans, or protocols in place to manage data security and privacy incidents that implicate personally identifiable information:

- The measures Happy Numbers has to ensure security are listed in Appendix A.
- In the event Happy Numbers becomes aware of an unauthorized disclosure or data breach:
- The District and teachers will be notified within 24 hours by email if the teacher account or any related student accounts are affected. The appropriate person in the school or school district who has purchased the valid school-wide or district-wide Happy Numbers access will be notified by phone if the users from this school or school district are affected.

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

9. Termination

Upon the termination of the agreement, Happy Numbers Inc. shall delete or destroy all information in its possession that is deemed to be confidential under the agreement with the District:

- by default, we will delete all confidential information, including the back-ups we and our trusted third parties hold, within 30 days after June 30th of the current calendar year.

- upon request, as explained in our terms of services, we will delete any confidential information within five days from our website and within 30 days from our trusted third parties.

The deletion from Google Cloud Servers occurs in phases, beginning with marking the data for deletion in active storage systems immediately and isolating the data from ordinary processing at the application layer. Successive compaction and mark-and-sweep deletion cycles in Google's storage layers serve to overwrite the deleted data over time. Cryptographic erasure is also used to render the deleted data unrecoverable. Finally, backup systems containing snapshots of Google's active systems are retired on a standard cycle.

Upon request by the District, we can transfer any personally identifiable information we hold to the school or its designated third party.

Email us with your requests at support@happynumbers.com

DocuSigned by:

CONTRACTOR: ____________________

0B1C4983C00645C...

Printed Name: Evgeny Milyutin
By: Title: Chief Executive Officer

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), a 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 occur if 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 with 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 laptop accounts and services
    - Password and/or fingerprint protection of all phones/tablets with access to any work data, including email

  - ○ No pass for 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 use for all applications, including app-to-app communication

General Application Security

- Check all security bulletins for used software (at the least NGINX, OpenVPN, Ruby on Rails, Postgresql, iptables, and others) and apply security patches accordingly.
- Regularly apply OS security updates on all servers.
- Keep each application in an isolated private network with its own VPN access.
- Staging and testing environments are located in separate private networks and use only anonymized databases or are filled with fake data.
- In all production environments, 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 (http://docs.ansible.com/ansible/playbooks_vault.html)

Data Breach Notification Policy

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.

If there is a valid reason to suspect a breach, Happy Numbers Inc. incident response team will:

- Check for common indicators of compromise to determine whether a breach has occurred.
- Conduct additional research as necessary to determine the extent of the impact.

Suppose it is determined that a breach has occurred. In that case, system(s) or system component(s) may need to be taken offline until they can be locked down with additional security measures (change passwords and certificates, update firewall settings, etc.)

An official statement will be issued to clients, summarizing our findings and providing an estimated time frame for service restoration.