Central Islip Union Free School District
Program Information and Data Privacy Third Party Agreement

To be completed **by the vendor** and submitted for all NEW and RENEWAL software/programs prior to purchase/implementation. Refusal of the vendor complete this agreement may serve as cause for the district to see similar services through another program and/or vendor. Failure to complete this form in its entirety will significantly delay any/all program purchases.

Software/Program Title:	Happy Numbers.com
Publisher:	Happy Numbers Inc.
Eastern Suffolk BOCES NYS Contract ☐ N/A Google App/Extension	☐BOCES Contract ☐BOCES CMR ☐BOCES Shared-Service ☐NYS Contract Pricing. Contract #: _____ ☐Federal Contract Pricing. Contract # _____ ☑No BOCES/NYS/Federal Contract – Direct Bid/RFP with Vendor
Account Management SSO/LDAP/SIS *Check all that apply* ☐ N/A Google App/Extension	☐SSO through LDAP/AD/ADFS ☐NO LDAP/AD/ADFS Option ☐Non SSO Centrally Managed (all Users) ☐Teachers Centrally Managed and create classes students ☑SIS/PowerSchool SSO/Directory User management ☐Non-User Based Program/Not Applicable
Platform ☐ N/A Google App/Extension	☐Local Install ☐Local Server/Network ☑100% Web-based ☐Web-Based with Local application/plug-in ☐Other/Explain: _____
Locations: ☐ N/A Google App/Extension	☑Elementary ☐Secondary ☐K-12 ☐Non-Educational Resource ☐Pilot in Specific Locations ☑Spanish Support/Spanish Language Offered
License Structure: ☐ N/A Google App/Extension	☐Per-User ☑Per-Student ☐Per-Classroom ☐Per-Teacher ☑Per-Building ☑Districtwide/Unlimited ☐Other/Explain: _____
License Renewal ☐ N/A Google App/Extension	☐Perpetual (no-renewal) ☑Annual ☐Other/Explain: _____
Separate Hosting Fees: ☐ N/A Google App/Extension	☑NO ☐YES - Annually ☐Other/Explain: _____

Contractor Initials: E.M.

Adobe Flash ☐ N/A Google App/Extension	☑Program DOES NOT require Adobe Flash ☐Program REQUIRES Adobe Flash If Yes please include implementation plan and details company roadmap and guarantee that all Adobe Flash will be transitioned to HTML5 prior to December 2020.
Configuration, Deployment, Initial Roll-Out Support ☐ N/A Google App/Extension	☐Full On-Site Support Included in the Proposal/Fee ☑Remote Support Only ☐Remote Support Included/On-Site for Additional Fees
Staff Training/Professional Development ☐ N/A Google App/Extension	☐Full On-Site Training/Development Included in the Proposal/Fee ☑Remote/WebEx Training/Development and Support Only ☐Combined On-Site/WebEx Training included in proposal
YouTube/Streaming Integration ☐ N/A Google App/Extension	☐Program requires full YouTube Access for linked Videos ☑All Program Videos/Media are native and NOT 3rd Party ☐Program DOES NOT require YouTube or N/A ☐Program Requires OTHER Streaming Site Access
Mobile Native APP iOS/Android ☐ N/A Google App/Extension	☐Available in the Appstore and Included ☐Available in the Appstore Additional Fees/License Fees ☑Not Available and/or No Native App
SIS-PowerSchool Integrations ☐ N/A Google App/Extension	☐Program DOES NOT sync to SIS (PowerSchool) ☑Program DOES sync to SIS (PowerSchool) ☐Not Applicable
Eastern Suffolk BOCES PowerSchool Support ☐ N/A Google App/Extension	☐Eastern Suffolk BOCES DOES Support PowerSchool Sync/Script ☐Eastern Suffolk BOCES DOES NOT (or Currently Does Not) Support PowerSchool Sync/Script ☑Not Applicable

Contractor Initials: E.M.

DATA PRIVACY AGREEMENT WITH THE CENTRAL ISLIP UNION FREE SCHOOL DISTRICT

Software Title:	HappyNumbers.com
Publisher/Developer:	Happy Numbers Inc.
Developer/Vendor Name	Happy Numbers Inc.
Developer/Vendor Mailing Address	billing@happynumbers.com
Developer/Vendor Privacy Policy Link:	https://happynumbers.com/privacy-policy
Developer/Vendor Parent Bill of Rights Link	N/A

This Data Privacy Agreement ("DPA") is by and between the Central Islip Union Free School District (herein known as "EA"), an Educational Agency, and the above listed software, app or extension developer (herein known as "Contractor"), collectively, the “Parties”.

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor’s security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** 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. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.

Contractor Initials: E.M.

6. **Eligible Student:** A student who is eighteen years of age or older.

7. **Encrypt or Encryption**: As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** 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 Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal prekindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** 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.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: 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 Education Law §§ 3012-c and 3012-d.

 Contractor Initials: E.M.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated below ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("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); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. Data Security and Privacy Plan.

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and

Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. EA's Data Security and Privacy Policy

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

Contractor Initials: E.M.

5. Right of Review and Audit.

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. Contractor's Employees and Subcontractors.

(a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

(b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

Contractor Initials: E.M.

7. Training.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

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. Data Return and Destruction of Data.

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction.

Redaction is specifically excluded as a means of data destruction.

(c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

 Contractor Initials: E.M.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

Philip K. Voigt
Director of Instructional Technology
50 Wheeler Rd
Central Islip, NY 11722
Pvoigt@centralislip.k12.ny.us

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

Contractor Initials: E.M.

14. **Notification to Individuals.**
Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. **Termination**.
The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.
Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA 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 EA and refer the Parent or Eligible Student to the EA.

2. **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 and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**
In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution.**
This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

Contractor Initials: E.M.

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. 65016502 (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-privacysecurity/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 EA's Director of Technology at pvoigt@centralislip.k12,ny.us
(ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/reportimproper-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. 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.

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

Contractor Initials: E.M.

EXHIBIT B

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

Description of the purpose(s) for which Contractor will receive/access PII	Description: The data is used to provide the functionality of the services. For more information, please, see our privacy policy: https://happynumbers.com/privacy-policy ☐ NO PII OR DATA IS COLLECTED OR VIEWABLE THROUGH THIS PROGRAM/APP
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR Data
Contract Term	Each Contract is valid through the software renewal period or 3 school years in the case of "Free" programs, apps, extensions and pilots.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: ☑ Securely transfer data to EA, or a successor contractor at the EA's 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 EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Encryption	☑ Data will be encrypted while in motion and at rest.

As the duly authorized officer of the "contractor" as listed above I attest to all of the above submitted information to be true and accept any liability and/or responsibility for any data breeches or intrusions associated with this program, applications, software or browser extension.

DocuSigned by:
0B1C4983C00645C...

Evgeny Milyutin, CEO

Signature of Vendor Official Representative

11/2/2022

Date

Signature must be an actual signature and cannot be a script font or text. If the program does not collect or transmit any PII, this document must still be completed, initialed (pages) and signed but you may and the select "NO PII OR DATA IS COLLECTED OR VIEWABLE" option above. No program/app/extension will be considered without a complete agreement.

Contractor Initials: E.M.

DATA SECURITY AND PRIVACY PLAN

Pursuant to 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), and the California Education Code including the Student Online Personal Information Protection Act (SOPIPA) and AB1584.

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 comply with the same.

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 confidentiality of such data. Such training shall be provided: for each employee on April 1 of each calendar year.

5. Happy Numbers Inc. shall utilize subcontractors and manage the relationships and contracts with such subcontractors in a way that ensures that subcontractors do the same as Happy Numbers or better job in protecting the data of Happy Numbers users. This includes reviewing existing terms of service, privacy policy of the subcontractor and signing additional agreements with the subcontractor if it's needed.

6. 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 is listed in Appendix A.
- In the event Happy Numbers become aware of an unauthorized disclosure or data breach:
- teachers will be notified 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.

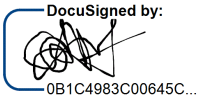
7. Termination

Upon the termination Happy Numbers Inc. shall delete or destroy all student data or teacher or principal data in its possession except for the information needed for archiving and that is publicly available:

- by default, we will delete all students' personally identifiable information we and our trusted third parties hold within 1 year after June 30th of the current calendar year.
- upon request, as explained in our terms of services, we will delete students' personally identifiable information within 5 days from our website and within 60 days from our trusted third parties.

Upon request by the district, we can transfer any students' personally identifiable information we held to the school or its designated third party. District can request such a transfer not more than once a year.

Email us with your requests at support@happynumbers.com

CONTRACTOR: 

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

11/2/2022

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

Data Breach Notification Policy

In the event we become aware of an unauthorized disclosure or data breach:

- teachers will be notified by email if the teacher account or any related student accounts are affected.

- 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.

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.