

## 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.

### **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 (IaC) 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:

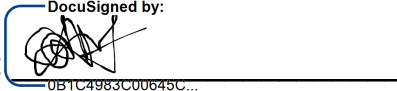
- by default, we will delete all confidential information, including the back-ups we and our trusted third parties hold, within 30 days after June 30th of the current calendar year.
- upon request, as explained in our terms of services, we will delete any confidential

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](mailto:support@happynumbers.com)

CONTRACTOR: 

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](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.