Baldwinsville Central School District
Achieving our full potential together.

DATA SECURITY AND PRIVACY PLAN

WHEREAS, the Baldwinsville Central School District (hereinafter "School District") and Humy (hereinafter "Contractor") entered into an agreement dated 11-8-2023 (hereinafter "Agreement") for Hello History (hereinafter "Services").

WHEREAS, pursuant to the requires under 8 NYCRR 121, Contractor maintains the data security and privacy plan described herein in connection with the Services provided to the School District.

1. During the term of the Agreement with the School District, Contractor 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):

Our organization employs several safeguards and practices to protect personally identifiable information (PII), in compliance with FERPA and CCPA regulations:

- Data Minimization: We process only the student data that is strictly necessary for our product's features, such as emails for login and cookies for app settings.
- Secure Infrastructure: We utilize Microsoft Azure's cloud services, known for their robust security measures and compliance certifications.
- Encryption: PII is secured using encryption both at rest and in transit.
- Parental Rights: We have mechanisms in place to ensure parents can access their children's educational records upon verified identity.
- Subcontractor Compliance: We mandate that our subcontractors' data processing agreements align with FERPA and CCPA.
- Disclosure Recordkeeping: We maintain records of disclosures as required by law.
- Incident Response: Our organization has prepared procedures for responding to potential PII data breaches.

2. Contractor has in place the following administrative, operational and technical safeguards and practices to protect personally identifiable information that it will receive under the Agreement:

To protect Personally Identifiable Information (PII), our organization implements the following measures:

- Least Privilege Access: We adhere to the principle of least privilege for IT systems access, ensuring only necessary personnel have access to sensitive data.
- Multi-Factor Authentication: Critical IT systems are secured using multi-factor authentication (MFA) to enhance data security.
- Password and API Key Management: We regularly rotate passwords and API keys to maintain security integrity.
- System Log Audits: We conduct weekly audits of system logs to monitor for any anomalies or suspicious activities.
- Ongoing Training: Our staff undergoes ongoing training on data security and privacy, conducted by our tech team, to stay updated on best practices and regulatory compliance.

3. Contractor 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 same.

a. Contractor will use the student data or teacher or principal data only for the exclusive purposes defined in the Agreement.

b. Contractor will ensure that the subcontractor(s) or other authorized persons or entities to whom Contractor will disclose the student data or teacher and principal data, if any, will abide by all applicable data protection and security requirements as described in the "Supplemental Information" appended to the Agreement.

c. At the end of the term of the Agreement, Contractor will destroy, and at the direction of the School District return, all student data and all teacher and principal data in accordance with the "Supplemental Information" appended to the Agreement.

d. Student data and teacher and principal data will be stored in accordance with the "Supplemental Information" appended to the Agreement.

e. Student data and teacher and principal data in motion and at rest will be protected using an encryption method that meets the standards described in 8 NYCRR 121.

4. Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of Contractor 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:

On November 2, 2023.

5. Subcontractors (check one):

□ Contractor shall not utilize sub-contractors.

☑ Contractor shall utilize sub-contractors. Contractor shall manage the relationships and contracts with such sub-contractors in the following ways in order to ensure personally identifiable information is protected:

- **Subcontractor Vetting**: We implement a stringent selection process, evaluating potential subcontractors for robust data security practices and compliance with relevant privacy regulations.
- **Binding Data Protection Agreements**: All subcontractors are contractually obligated to adhere to strict data protection clauses, ensuring PII is handled in compliance with legal standards.
- **Compliance Monitoring**: We conduct periodic audits of subcontractor operations to verify ongoing adherence to data protection policies.
- **Mandatory Data Security Training**: Subcontractors are required to participate in comprehensive training programs focusing on PII confidentiality and compliance with data security laws.
- **Incident Reporting Procedures**: We have established protocols for immediate notification and response in the event of any data security incidents.
- **Controlled Data Access**: Access to PII is strictly governed by need-to-know principles, ensuring minimal exposure of sensitive information.
- **Enforcement of Encryption Protocols**: We mandate the use of industry-standard encryption methods for PII, both at rest and in transit.
- **Secure Data Disposal Post-Engagement**: Clear procedures are set for the secure disposal or return of PII upon termination of subcontractor services.

6. Contractor has the following procedures, plans or protocols in place to manage data security and privacy incidents that implicate personally identifiable information: *Procedures, plans or protocols must, at a minimum, specify plans to identify breaches and unauthorized disclosures, and to promptly notify the School District.*

Our organization has established comprehensive procedures, plans, and protocols to effectively manage data security and privacy incidents that implicate PII. These include:

- **Incident Identification and Assessment**: We have procedures in place for the early detection and assessment of potential breaches and unauthorized disclosures of PII. **Incident Response Plan**: Upon identification of a potential incident, our incident response procedure is activated. The CTO is responsible for containing the incident, assessing its impact, and initiating recovery measures.
- **Notification Protocol**: In the event of a confirmed breach or unauthorized disclosure of PII, we have a protocol to promptly notify the School District. This notification includes details of the incident, the type of data involved, the estimated number of individuals affected, and the steps taken to mitigate the incident.
- **Ongoing Communication**: Following the initial notification, we maintain regular communication with the School District, providing updates on the incident investigation, the measures taken to secure the data, and steps for preventing future occurrences.
- **Documentation and Review**: All incidents are thoroughly documented, and post-incident reviews are conducted to analyze the cause and effectiveness of the response. Lessons learned are integrated into our ongoing risk management and security practices.
- **Compliance with Legal Requirements**: Our procedures align with federal and state laws governing the confidentiality and security of PII, ensuring that all legal obligations are met in the event of an incident.

7. Termination of Agreement.

   a. Within 30 days of termination of the Agreement, Contractor shall delete or destroy all student data or teacher or principal data in its possession; AND

b. Within 15 days of termination of the Agreement, Contractor shall Returned all data to the School District using using secure, encrypted digital transfer methods. This may include secure file transfer protocol (SFTP) or an encrypted file-sharing service.; OR Transition all data to a successor contractor designated by the School District in writing using secure file transfer protocol (SFTP) or an equivalent encrypted file-sharing service.

8. In the event of a conflict between the terms of this Data Security and Privacy Plan and the terms of the Agreement, the terms of this Data Security and Privacy Plan shall control. All of the defined terms in the Agreement shall have the same definitions in the Data Security and Privacy Plan, unless otherwise defined herein. Except as expressly set forth in this Data Security and Privacy Plan, the terms and conditions of the Agreement shall remain unmodified and in full force and effect.

IN WITNESS WHEREOF, the Contractor hereto has executed this Data Security and Privacy Plan as of 11.11.2023.

CONTRACTOR:
FACING IT International AB
By: Martin Balodis
Title: CEO

Audit Trail

Document Details

Title	Bville Vendor Contract-Humy
File Name	Bville Vendor Contract-Humy.docx.pdf
Document ID	bf4f036ae32c4734911b0628fd86b665
Fingerprint	459c4d0b408f9ff6197c393b72f62d81
Status	Completed

Document History

Document Created	Document Created by Martin Balodis (martin@facing-it.com) Fingerprint: 9e7202b44d6238323662489a4924154b	Nov 13 2023 07:46AM UTC
Document Signed	Document Signed by Martin Balodis (martin@facing-it.com) IP: 90.129.242.243 	Nov 13 2023 07:46AM UTC
Document Completed	This document has been completed. Fingerprint: 459c4d0b408f9ff6197c393b72f62d81	Nov 13 2023 07:46AM UTC