# DATA SECURITY & PRIVACY POLICY

## I. Overview

This Data Security and Privacy Policy describes the policies and procedures of Press4Kids Inc. (P4K) with respect to data security and privacy and especially the information collected by P4K through its product News-O-Matic and the protection of such information. Press4Kids requires that its subcontractors that receive PII (defined below) maintain similar policies.

Press4Kids has appointed a Chief Information and Security Officer (CISO) responsible for developing, implementing and maintaining this Data Privacy and Security Policy, under the oversight of Press4Kids's Chief Executive Officer.

## II. Definitions

Any capitalized term used within this DSPP will have the meanings as defined below:

(a) "Personally Identifiable Information" or "PII" means personally identifiable information as defined in FERPA or relevant state law, i.e. any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for deanonymizing previously anonymous data can be considered PII.

(b) "Student Data" means students PII collected from an Educational Agency.

(c) "Teacher or Administrators Data" means teachers and Education Agency administrators (such as principal or librarian) collected from an Educational Agency.

(c) "Protected Data" means Student Data and/or Teacher or Administrator Data to the extent applicable to Press4Kids' Product.

(d) "Educational Agency" means a school or a district which is licensed to use Press4Kids' Product.

(e) "Breach" means the unauthorized acquisition, access, use, or disclosure of PII which compromises the security or privacy of such information.

(f) " “Destroy” means to remove PII so that it is permanently irretrievable in the normal course of business.

(g) “FERPA” means the Family Educational Rights and Privacy Act of 1974 (codified at 20 U.S.C. § 1232g) and its implementing regulations, issued by the U.S. Department of Education, and available at http://www2.ed.gov/policy/gen/reg/ferpa/index.html.

(h) "Subcontractor" means contractor of P4K that may be required to maintain or handle PII collected by P4K from an Educational Agency

(i) "Security Incident" is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices or an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies

Security Incidents may include a Breach or hacking of the Press4Kids Electronic Data System or any loss or theft of data, other electronic storage, or paper. As used herein, "Electronic Data System" means all information processing and communications hardware and software employed in Press4Kids’s business, whether owned by Press4Kids or operated by its employees, agents or Subcontractors in performing work for Press4Kids.

**III. USE OF PERSONALLY IDENTIFIABLE INFORMATION BY PRESS4KIDS**.

Student Personally Identifiable Information ("PII") may be provided by customers and used by Press4Kids to perform contracted services and to carry out studies designed to improve the Press4Kids offering and the customer experience.

Student Data is never shared without written authority from the customer unless Press4Kids is legally required to do so by subpoena or court order. Disclosure of PII to Press4Kids is authorized by the Family Educational Rights and Privacy Act ("FERPA") only for the purposes of performing institutional services for the customer as a “school official” pursuant to the conditions and restrictions set forth in § 99.31 (a) (1) (i) (B).

Press4Kids collects only the student data required to operate its service. Personal identifiable student data is not shared with third parties for marketing purposes. Our student PII collection is limited to a Unique Identifier (does not need to be tied to a name but the teacher needs to know which student it belongs to).

Press4Kids also collects teacher and administrators emails.

**Customer Ownership of the Data**. All data provided to Press4Kids by customers, including student data, remains the property and responsibility of customers in accordance with FERPA and applicable state law. As such, each customer is responsible for ensuring its own compliance with applicable law, including FERPA.

## IV. PRIVACY OF PERSONAL INFORMATION

### A. Privacy Protections

1. *Compliance with Law and Policy*. All PII uploaded to or made accessible to Press4Kids is handled, processed, stored, transmitted and protected in accordance with all applicable federal data privacy and security laws (including FERPA), data privacy and security laws of the state from which the data originated, and with this Policy. Press4Kids designs and maintains its programs, systems and infrastructure with respect to the receipt, maintenance and sharing of Protected Data to comply with all applicable data security and privacy requirements arising out of state, federal, and local law. Our Chief Information and Security Officer (CISO) tracks those requirements and maintains compliance by ensuring that privacy and security are elements of all design and redesign efforts, and through ongoing internal systems reviews and updates.

This document details measures taken by Press4Kids to (i) secure Protected Data and to limit access thereto (ii) implement "best practices" and industry standards with respect to data storage, privacy and protection, including, but not limited to encryption, firewalls, passwords, protection of off-site records, and limitations of access to stored data to authorized staff, and (iii) ensure that subcontractors, if any, receiving Protected Data, if any, will abide by the legal and contractual obligations with respect to Student Data.

2. *Training*. Employees of Press4Kids (including temporary and contract employees) are annually educated and trained on the proper uses and disclosures of PII and the importance of information privacy and security.

3. *Employees Guidelines*. All Press4Kids employees are required to be aware of and work to protect the confidentiality, privacy, and security of PII. Press4Kids and its employees do not access PII except to comply with a legal obligation under federal or state law, regulation, subpoena, or action by a customer that requires such access, or where they have a legitimate need for the information to maintain their data system or perform services for customers as contractually agreed upon. The following list provides a general description of internal Press4Kids policies:

1. Limit internal access to PII to Press4Kids and its employees with proper authorization and allow use and/or disclosure internally, when necessary, solely to employees with a legitimate need for the PII to carry out the educational purposes of Press4Kids under its contracts with customers.

2. Allow access to PII in Press4Kids's possession by parties other than the customer only where users are authorized to have access to PII by the customer.
3. Require that materials containing PII in electronic form are stored solely within encrypted data repositories and PII are not available on unencrypted shared drives or on a local drive.
4. When PII is no longer needed or customers request the return of PII, delete access to PII, in accordance with secure destruction procedures.
5. Permit Press4Kids employees to download information onto storage only as directed by Press4Kids's CISO and ensure that the information is encrypted and stored in password-protected files, and that devices containing the information have appropriate security settings in place (such as encryption, firewall protection, anti-virus software and malware protection).
6. Require that any downloaded materials consisting of PII remain in the United States.

**V. INFORMATION SECURITY PROGRAM**

**Access to PII**

1. *Customer -- access to PII*. Customers that provide access to PII to Press4Kids may contractually determine access to PII for parties beyond Press4Kids and its employees.

2. *Parent Inquiries*. Press4Kids cooperates with the customer in addressing inquiries or complaints from parents (or students 18 and over) that relate to their use or disclosures of PII.

Press4Kids's IT Security Plan consists of technical, physical, and administrative safeguards to protect PII. This plan includes the following key general processes:

**A. Information Security Risk Assessment**

Press4Kids CISO periodically conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic, paper, or other records containing PII maintained by Press4Kids; the CISO reports such risks as promptly as possible to Press4Kids' leadership team or other official within Press4Kids designated to be responsible for data privacy and security compliance; and implements security measures sufficient to reduce identified risks and vulnerabilities. Such measures are implemented based on the level of risks, capabilities, and operating requirements. These measures must include as appropriate and reasonable the following safeguards:

**1. Administrative Safeguards**

i. *Discipline*: Press4Kids enacts appropriate discipline with respect to employees who fail to comply with Press4Kids security policies and procedures.
ii. *System Monitoring*: Press4Kids maintains procedures to regularly review records of information systems activity, including maintaining access logs, access reports, security incident tracking reports, and periodic access audits.
iii. *Security Oversight*: Press4Kids CISO is responsible for developing, implementing, and monitoring of safeguards and security issues.
iv. *Appropriate Access*: Procedures to determine that the access of Press4Kids employees to PII is appropriate and meets a legitimate need to support their roles in business or educational operations. Procedures for establishing appropriate authorization and authentication mechanisms for Press4Kids employees who have access to PII.
v. *Access Termination*: Procedures for terminating access to PII when employment ends, or when an individual no longer has a legitimate need for access.

**2. Access Safeguards**

i. *Access to PII*: Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.
ii. *Awareness Training*: On-going security awareness through training or other means that provide Press4Kids employees (including management) with updates to security procedures and policies (including guarding against, detecting, and reporting malicious software). Awareness training should also address procedures for safeguarding passwords.
iii. *Incident Response Plan*: Procedures for responding to, documenting, and mitigating where practicable suspected or known incidents involving a possible breach of security and their outcomes.
iv. *Encryption and Final Disposition of Information*: Procedures addressing encryption of all data at rest and in transit and the final disposition of PII. Procedures must include processes for the continued encryption of customer's PII through the time when its secure deletion/destruction has been requested in writing by the customer, or when the terms of the agreement between Press4Kids and a customer require that the PII be deleted/destroyed.

**3. Technical Safeguards**

i. *Access to PII*: Procedures that grant access to PII by establishing, documenting, reviewing, and modifying a user's right of access to a workstation, software application/transaction, or process.
ii. *Awareness Training*: On-going security awareness through training or other means

iii. *Data Transmissions*: Technical safeguards to ensure PII transmitted over an electronic communications network is not accessed by unauthorized persons or groups. Encryption is used when PII are in transit or at rest. Unencrypted PII is not transmitted over public networks to third parties.
iv. *Data Integrity*: Procedures that protect PII maintained by Press4Kids from improper alteration or destruction. These procedures include mechanisms to authenticate records and corroborate that they have not been altered or destroyed in an unauthorized manner.

4. **Data Storage:**
Press4Kids collects only the data required to operate the service. PII data is not shared with third parties for marketing purposes.

5. **Code Access Control**
Press4Kids source code is stored in private password protected repositories. Repository access is approved by CISO. Press4Kids repositories may be available to contracted engineers on an as-needed and temporary basis. Contractors may not receive access to repositories without cause and without being signatories to Press4Kids's contracting agreement. Access is revoked upon lapse of contract.

**6. Infrastructure**

i. *Hosting* All production application infrastructure is hosted by a Third-Party Services. Hosting providers must provide materials to Press4Kids documenting rigorous security and data privacy practices.
ii. *Firewalls & Network Isolation* All production and staging servers are hosted inside of a Virtual Private Cloud. Press4Kids does not own or co-locate servers for its applications. Press4Kids does not maintain on- premise application infrastructure. Application production and staging networks are isolated from business networks.
iii. *Credentials* Press4Kids engineers are granted access to services by the principle of least-privilege-required upon onboarding, and permissions and users are audited monthly. Requests for new permissions must be submitted to senior management. Removal of credentials is part of off-boarding procedure when employment is terminated. Contracted personnel are not permitted to have credentials to production assets.
iv. *Encryption* HTTPS via SSL is required to connect to all web servers from the public network. Application database is encrypted-at-rest.

**B. Security Controls Implementation**

Press4Kids has procedures addressing the acquisition and operation of technology, the specific assignment of duties and responsibilities to managers and staff, the deployment of risk-appropriate controls, and the need for management and staff to understand their

responsibilities and have the knowledge, skills and motivation necessary to fulfill their duties.

**C. Security Monitoring & Improvement**

Press4Kids uses a variety of approaches and technologies to make sure that risks and incidents are appropriately detected, assessed and mitigated on an ongoing basis. Press4Kids assesses on an ongoing basis whether controls are effective and performing as intended.

Based on Press4Kids's security risk assessments and ongoing security monitoring, Press4Kids gathers and analyzes information regarding new threats and vulnerabilities, actual data attacks on Press4Kids, and new opportunities for managing security risks and incidents. Press4Kids uses this information to update and improve its risk assessment strategy and control processes.

**D. Incident Response**

Press4Kids has a formal Incident Response plan but due to its sensitive nature Press4Kids does not provide details outside of the company.

Press4Kids employees are required to report any Security Incident, or suspected Security incident, of which they become aware as promptly as possible to Press4Kids CISO.

If Press4Kids determines that a Breach has occurred, Press4Kids will notify affected customers promptly and will cooperate with customers as needed to enable compliance with all state breach of confidentiality laws.

**E. Personnel Security Policy Overview**

Press4Kids mitigates the risks posed by internal users of PII by:

1. Performing appropriate background checks and screening of Press4Kids employees, who are granted access to Press4Kids - maintained PII;
2. Obtaining agreement from Press4Kids internal users as to confidentiality, nondisclosure and authorized use of PII; and
3. Providing training to support awareness and policy compliance for new hires and annually for all Press4Kids employees.