

## EXHIBIT D

### **VI. Exhibits**

#### **VI.A. Data Privacy Agreement**

##### DATA PRIVACY AGREEMENT

INCLUDING

PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY AND  
SUPPLEMENTAL INFORMATION ABOUT THE Agreement

#### **1. Purpose**

(a) This Data Privacy Agreement (DPA) supplements the agreement between Capital Region BOCES (BOCES) and Press4Kids, to ensure that the Vendor AGREEMENT conforms to the requirements of New York State Education Law Section 2-d and any implementing Regulations of the Commissioner of Education (collectively referred to as "Section 2-d"). This Agreement consists of the terms of this DPA Agreement, a copy of BOCES Parents' Bill of Rights for Data Security and Privacy signed by Press4Kids, and the Supplemental Information about the AGREEMENT that is required to be posted on BOCES website.

(b) To the extent that any terms contained within the Purchase AGREEMENT, or any terms contained within any other Agreements attached to and made a part of the Vendor AGREEMENT, conflict with the terms of this DPA, the terms of this DPA will apply and be given effect. In the event that Press4Kids has online or written Terms of Service ("TOS") that would otherwise be applicable to its customers or users of its Product that is the subject of the Purchase AGREEMENT, to the extent that any term of the TOS conflicts with the terms of this DPA, the terms of this DPA will apply and be given effect.

#### **2. Definitions**

Any capitalized term used within this DPA that is also found in the Purchase AGREEMENT will have the same definition as contained within this DPA.

In addition, as used in this Exhibit:

(a) "Student Data" means personally identifiable information, as defined in Section 2-d, from student records that Press4Kids receives from a Participating Educational Agency pursuant to the DPA.

(b) "Teacher or Principal Data" means personally identifiable information relating to the annual professional performance reviews of classroom teachers or principals

that is confidential and not subject to release under the provisions of New York Education Law Sections 3012-c or 3012-d, that Press4Kids receives from a Participating Educational Agency pursuant to the Purchase AGREEMENT.

(c) "Protected Data" means Student Data and/or Teacher or Principal Data to the extent applicable to Press4Kids' Product (News-O-Matic).

(d) "Participating Educational Agency" means a school district within New York State that purchases certain shared instructional technology services and software through a Cooperative Educational Services Agreement with BOCES, and as a result is licensed to use Press4Kids'S Product pursuant to the terms of the AGREEMENT.

### **3. Confidentiality of Protected Data**

(a) Press4Kids acknowledges that the Protected Data it receives pursuant to the AGREEMENT may originate from several Participating Educational Agencies located across New York State, and that this Protected Data belongs to and is owned by the Participating Educational Agency from which it originates.

(b) Press4Kids will maintain the confidentiality of the Protected Data it receives in accordance with federal and state law (including but not limited to Section 2-d) and BOCES policy on data security and privacy. Press4Kids acknowledges that BOCES is obligated under Section 2-d to adopt a policy on data security and privacy, and has provided the policy to Press4Kids.

### **4. Data Security and Privacy Plan**

Press4Kids agrees that it will protect the confidentiality, privacy and security of the Protected Data received from Participating Educational Agencies in accordance with the BOCES Parents' Bill of Rights for Data Privacy and Security, a copy of which has been signed by Press4Kids and is set forth below.

Additional elements of Press4Kids' Data Security and Privacy Plan are as follows:

(a) In order to implement all state, federal, and local data security and privacy requirements; including those contained within this DPA, consistent with BOCES data security and privacy policy, Press4Kids will:

Press4Kids Data Security and Privacy Plan is fully consistent with BOCES Security and Privacy Policy and follows the state, federal and local requirements.

Press4Kids does not store any PII except teacher's and administrator's email to access News-O-Matic. Students' PII are not requested or needed. No data are shared outside of Press4Kids. Data storage is done on Press4Kids' protected servers, hosted on Amazon Web Services.

(b) In order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Purchase AGREEMENT, Press4Kids will have the

following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Purchase AGREEMENT:

Press4Kids uses and maintains security protocols that meet industry best practices in the transfer or transmission of data, including ensuring that data may only be viewed or accessed by parties legally allowed to.

SSL technology is employed to protect data. Data encryption and secured authentication are implemented.

Press4Kids will provide Participating Educational Agency with contact information of an employee that can be contacted if there are any security concerns or questions.

(c) Press4Kids will comply with all obligations set forth in BOCES "Supplemental Information about the AGREEMENT" below.

(d) For any of its officers or employees (or officers or employees of any of its subcontractors or assignees) who have access to Protected Data, Press4Kids has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows:

- Periodic training for the Press4Kids employee on security, data protection and confidentiality
- Additional confidentiality agreement signed by this employee regarding said Protected Data
- Employees with access to Protected Data shall pass criminal background checks.

(e) Press4Kids will utilize sub-contractors for the purpose of fulfilling one or more of its obligations under the Purchase AGREEMENT. In the event that Press4Kids engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Purchase AGREEMENT, it will require such subcontractors, assignees, or other authorized agents to execute written agreements as more fully described in BOCES "Supplemental Information about the Purchase AGREEMENT," below.

(f) Press4Kids will manage data security and privacy incidents that implicate Protected Data, including identify breaches and unauthorized disclosures, and Press4Kids will provide prompt notification of any breaches or unauthorized disclosures of Protected Data in accordance with Section 6 of this Data Sharing and Confidentiality Agreement.

(g) Press4Kids will implement procedures for the return, transition, deletion and/or destruction of Protected Data at such time that the AGREEMENT is terminated or expires, as more fully described in BOCES "Supplemental Information about the AGREEMENT," below.

## **5. Additional Statutory and Regulatory Obligations**

Press4Kids acknowledges that it has the following additional obligations with respect to any Protected Data received from Participating Educational Agencies, and

that any failure to fulfill one or more of these statutory or regulatory obligations shall be a breach of the **Purchase AGREEMENT** and the terms of this Data Sharing and Confidentiality Agreement:

(a) Limit internal access to education records to those individuals that are determined to have legitimate educational interests within the meaning of Section 2-d and the Family Educational Rights and Privacy Act (FERPA).

(b) Limit internal access to Protected Data to only those employees or subcontractors that need access in order to assist **Press4Kids** in fulfilling one or more of its obligations under the **Purchase AGREEMENT**.

(c) Not use education records for any purposes other than those explicitly authorized in this Data Sharing and Confidentiality Agreement.

(d) Not disclose any personally identifiable information to any other party, except for authorized representatives of **Press4Kids** using the information to carry out **Press4Kids**'s obligations under the **Purchase AGREEMENT**, unless:

1. (i) the parent or eligible student has provided prior written consent; or
2. (ii) the disclosure is required by statute or court order and notice of the disclosure is provided to Participating Educational Agency no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order.

(e) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable student information in its custody;

(f) Use encryption technology that complies with Section 2-d, as more fully set forth in BOCES "Supplemental Information about the **Purchase AGREEMENT**," below.

(g) Provide notification to BOCES (and Participating Educational Agencies, to the extent required by, and in accordance with, Section 6 of this Data Sharing and Confidentiality Agreement) of any breach of security resulting in an unauthorized release of Protected Data by **Press4Kids** or its assignees or subcontractors in violation of state or federal law or other obligations relating to data privacy and security contained herein.

(h) Promptly reimburse BOCES, another BOCES, or a Participating School District for the full cost of notification, in the event they are required under Section 2-d to notify affected parents, students, teachers or principals of a breach or unauthorized release of Protected Data attributed to **Press4Kids** or its subcontractors or assignees.

## **6. Notification of Breach and Unauthorized Release**

(a) Press4Kids shall promptly notify BOCES of any breach or unauthorized release of Protected Data in the most expedient way possible and without unreasonable delay, but no more than seven (7) calendar days after Press4Kids has discovered or been informed of the breach or unauthorized release.

(b) Press4Kids will provide such notification to BOCES by contacting the BOCES Data Privacy Officer, at [michele.jones@neric.org](mailto:michele.jones@neric.org).

(c) Press4Kids will cooperate with BOCES and provide as much information as possible directly to the Data Protection Officer (DPO) or designee about the incident, including but not limited to: a description of the incident, the date of the incident, the date Press4Kids discovered or was informed of the incident, a description of the types of personally identifiable information involved, an estimate of the number of records affected, the Participating Educational Agencies affected, what Press4Kids has done or plans to do to investigate the incident, stop the breach and mitigate any further unauthorized access or release of Protected Data, and contact information for Press4Kids representatives who can assist affected individuals that may have additional questions.

(d) Press4Kids acknowledges that upon initial notification from \_\_\_\_\_, BOCES, as the educational agency with which Press4Kids contracts, has an obligation under Section 2-d to in turn notify the Chief Privacy Officer in the New York State Education Department ("CPO"). Press4Kids shall not provide this notification to the CPO directly. In the event the CPO contacts Press4Kids directly or requests more information from Press4Kids regarding the incident after having been initially informed of the incident by BOCES, Press4Kids will promptly inform the Data Protection Officer or designees.

(e) Press4Kids will consult directly with the Data Protection Officer or designees prior to providing any further notice of the incident (written or otherwise) directly to any other BOCES or Regional Information Center, or any affected Participating Educational Agency.

BY Russell Kahn, Chief Content Officer, 11/02/2020,



## PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Albany-Schoharie-Schenectady-Saratoga BOCES (BOCES) is committed to protecting the privacy and security of personally identifiable information about students who attend BOCES instructional programs in accordance with applicable law, including New York State Education Law Section 2-d.

To further these goals, BOCES wishes to inform parents of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record, including any student data maintained by the Capital Region BOCES. This right of inspection of records is consistent with the federal Family Educational Rights and Privacy Act (FERPA). Under the more recently adopted regulations (Education Law §2-d), the rights of inspection are extended to include data, meaning parents have the right to inspect or receive copies of any data in their child's educational record. The New York State Education Department (SED) will develop further policies and procedures related to these rights in the future.

Requests to inspect and review a child's education record should be directed to: Data Privacy Officer, michele.jones@neric.org, 900 Watervliet-Shaker Road, Albany, NY 12205.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) 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 by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints may be directed to the NYS Chief Privacy Officer by writing to the New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be directed to the Chief Privacy Officer via email at: [CPO@mail.nysed.gov](mailto:CPO@mail.nysed.gov).

**BY** Russell Kahn, Chief Content Officer, 11/02/2020,



## SUPPLEMENTAL INFORMATION ABOUT THE AGREEMENT BETWEEN

### Albany-Schoharie-Schenectady- Saratoga BOCES AND Press4Kids

BOCES has entered into An Agreement (“AGREEMENT”) with Press4Kids (“\_\_\_\_\_”), which governs the availability to Participating Educational Agencies of the following Product(s): **News-O-Matic**

Pursuant to the AGREEMENT, Participating Educational Agencies may provide to Press4Kids and Press4Kids will receive, personally identifiable information about students, or teachers and principals, that is protected by Section 2-d of the New York State Education Law (“Protected Data”).

#### **Exclusive Purpose for which Protected Data will be Used:**

Press4Kids agrees that it will not use the Protected Data for any other purposes not explicitly authorized in the AGREEMENT. Protected Data received by Press4Kids, or any of Press4Kids’s subcontractors, assignees, or other authorized agents, will not be sold, or released or used for any commercial or marketing purposes.

**Oversight of Subcontractors:** In the event that Press4Kids engages subcontractors, assignees, or other authorized agents to perform one or more of its obligations under the AGREEMENT (including any hosting service provider), it will require those to whom it discloses Protected Data to execute legally binding agreements acknowledging the obligation under Section 2-d of the New York State Education Law to comply with the same data security and privacy standards required of Press4Kids under the AGREEMENT and applicable state and federal law.

Press4Kids will ensure that such subcontractors, assignees, or other authorized agents abide by the provisions of these agreements by:

Press4Kids

#### **Duration of AGREEMENT and Protected Data Upon Expiration:**

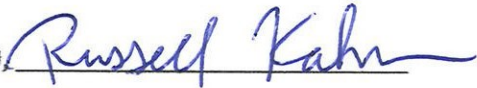
- The AGREEMENT commences on [date] and expires on [date]. Upon expiration of the AGREEMENT without renewal, or upon termination of the AGREEMENT prior to expiration, Press4Kids will securely delete or otherwise destroy any and all Protected Data remaining in the possession of Press4Kids or its assignees or subcontractors. If requested by a Participating Educational Agency, Press4Kids will assist that entity in exporting all Protected Data previously received for its own use, prior to deletion.
- At BOCES request, Press4Kids will cooperate with BOCES as necessary in order to transition Protected Data to any successor Press4Kids prior to deletion.
- Press4Kids agrees that neither it nor its subcontractors, assignees, or other authorized agents will retain any copy, summary or extract of the Protected Data, or any de-identified Protected Data, on any storage medium whatsoever. Upon request, Press4Kids and/or its subcontractors, assignees, or other authorized agents will provide a certification from an appropriate officer that these requirements have been satisfied in full.

**Challenging Accuracy of Protected Data:** Parents or eligible students can challenge the accuracy of any Protected Data provided by a Participating Educational Agency to Press4Kids by contacting the student's district of residence regarding procedures for requesting amendment of education records under the Family Educational Rights and Privacy Act (FERPA). Teachers or principals may be able to challenge the accuracy of APPR data provided to Press4Kids by following the appeal process in their employing school district's applicable APPR Plan.

**Data Storage and Security Protections:** Any Protected Data Press4Kids receives will be stored on systems maintained by Press4Kids or by a subcontractor under the direct control of Press4Kids in a secure data center facility located within the United States. The measures that Press4Kids 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 of Protected Data:** Press4Kids (or, if applicable, its subcontractors) will protect Protected Data in its custody from unauthorized disclosure while in motion or at rest, using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under Section 13402(H)(2) of P.L. 111-5.

**BY** Russell Kahn, Chief Content Officer, 11/02/2020





# 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.




## Parents Bill Of Rights for Vendors Working With Capital Region BOCES

Albany-Schoharie-Schenectady-Saratoga BOCES (Capital Region BOCES), in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. BOCES establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.
- A student's personally identifiable information cannot be sold or released for any marketing or commercial purposes by BOCES or any a third party contractor. BOCES will not sell student personally identifiable information and will not release it for marketing or commercial purposes, other than directory information released by BOCES in accordance with BOCES policy;
- Parents have the right to inspect and review the complete contents of their child's education record (for more information about how to exercise this right, see 5500-R);
- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
- A complete list of all student data elements collected by the State Education Department is available for public review at <http://nysed.gov/data-privacy-security> or by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to the Data Protection Officer, 518-464-5139, [DPO@neric.org](mailto:DPO@neric.org), Capital Region BOCES, 900 Watervliet-Shaker Rd., Albany NY 12205. Complaints can also be directed to the New York State Education Department online at <http://nysed.gov/data-privacy-security> by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to [privacy@mail.nysed.gov](mailto:privacy@mail.nysed.gov) or by telephone at 518-474-0937.
- Parents have the right to be notified in accordance to applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.
- Parents can expect that educational agency workers who handle PII will receive annual training on applicable federal and state laws, regulations, educational agency's policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

In the event that BOCES engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting the Data Protection Officer, 518-464-5139, [DPO@neric.org](mailto:DPO@neric.org), 900 Watervliet-Shaker Rd., Albany NY 12205, or can access the information on the Capital Region BOCES website [www.capitalregionboces.org](http://www.capitalregionboces.org).

Vendor/Company Name: Press4Kids Inc. (Product: News-O-Matic)  
Signature: Marcus Magdelenat   
Title: CEO  
Date: 12/20/21



Vendor Questionnaire (Data Privacy Agreement): 279685  
 Created Date: 12/6/2021 10:44 AM Last Updated: 12/21/2021 2:54 PM


### Directions

Below is the Third Party contact that will fill out the Part 121//DPA questionnaire. If this is accurate, click the blue "Publish" button. If not, select the appropriate contact by clicking "Lookup" or create a new contact by clicking "Add New".

### Vendor Compliance Contacts

Name (Full)	Email	Phone	Third Party Profile
Brandon Cohen	brandon@newsomatic.org		Press4Kids Inc. - News-O-Matic
James Baker	jim@newsomatic.org		Press4Kids Inc. - News-O-Matic
Russell Khan	russ@newsomatic.org		Press4Kids Inc. - News-O-Matic
Brandon C	b.cohen@fioptics.com		Press4Kids Inc. - News-O-Matic

### General Information

<b>Third Party Profile:</b>	Press4Kids Inc. - News-O-Matic	<b>Overall Status:</b>	Approved
<b>Questionnaire ID:</b>	279685	<b>Progress Status:</b>	 100%
<b>Engagements:</b>	Press4Kids - News-O-Matic (DREAM) 22-23	<b>Portal Status:</b>	Vendor Submission Received
<b>Due Date:</b>	12/21/2021	<b>Submit Date:</b>	12/20/2021
		<b>History Log:</b>	<a href="#">View History Log</a>

### Review

<b>Reviewer:</b>	CRB Archer Third Party: Risk Management Team	<b>Review Status:</b>	Approved
		<b>Review Date:</b>	12/21/2021

#### Reviewer Comments:

**Unlock Questions for Updates?:** Assessment questions are set to read-only by default as the assessment should be completed by a vendor through the vendor portal. Do you need to unlock the questionnaire to manually make an update to the submitted questions? This field should be reset to null after the update is made, prior to existing the record.

### Data Privacy Agreement and NYCRR Part 121

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

- 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.
- 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.
- 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.
- 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.
- 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.
- Eligible Student:** A student who is eighteen years of age or older.
- 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 pre-kindergarten 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.

<p><b>NYCRR - 121.3(b)(1):</b> What is the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?</p>	<p>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 administrator's emails.</p>
<p><b>NYCRR - 121.3(b)(2):</b> Will the organization use subcontractors? If so, how will the organization ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., FERPA; Education Law section 2-d, NIST Cybersecurity Framework)?</p>	<p>Press4kids will ensure that subcontractors, if any, receiving Protected Data, if any, will abide by the legal and contractual obligations with respect to Student, Teacher and Administrator Data.</p>
<p><b>NYCRR - 121.3(b)(3):</b> What is the duration of the contract including the contract's expected commencement and expiration date? If no contract applies, describe how to terminate the service. Describe what will happen to the student data or teacher or principal data upon expiration. (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be securely destroyed and how all copies of the data that may have been provided to 3rd parties will be securely destroyed)</p>	<p>1-year PII will either be either returned in a secure manner or destroyed using crypto shredding process</p>
<p><b>NYCRR - 121.3(b)(4):</b> How can a parent, student, eligible student, teacher or principal challenge the accuracy of the student data or teacher or principal data that is collected?</p>	<p>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. They need to send an email to <a href="mailto:info@newsomatic.org">info@newsomatic.org</a>.</p>
<p><b>NYCRR - 121.3(b)(5):</b> Describe where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.</p>	<p>Data will be encrypted and stored in a virtual private cloud, 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</p>

	(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	
<b>NYCRR - 121.3(b)(6):</b>	Please describe how and where encryption is leveraged to protect sensitive data at rest and while in motion. Please confirm that all encryption algorithms are FIPS 140-2 compliant.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.6(a):</b>	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	Data Security and Privacy Policy-2022.pdf
<b>NYCRR - 121.6(a)(1):</b>	Describe how the organization will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.6(a)(2):</b>	Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the engagement. If you use 3rd party assessments, please indicate what type of assessments are performed.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.6(a)(4):</b>	Specify how officers or employees of the organization and its assignees who have access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.6(a)(5):</b>	Specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.6(a)(6):</b>	Specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.6(a)(7):</b>	Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires. Vendor will be required to complete a Data Destruction Affidavit upon termination of the engagement.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.9(a)(1):</b>	Is your organization compliant with the <a href="#">NIST Cyber Security Framework?</a>	Yes
<b>NYCRR - 121.9(a)(2):</b>	Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law section 2-d; and this Part.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.9(a)(3):</b>	Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need authorized access to provide services.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.9(a)(4):</b>	Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract. (e.g. Role Based Access, Continuous System Log Monitoring/Auditing)	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.9(a)(5):</b>	Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i)except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with State and Federal law, regulations and its contract with the educational agency; or (ii)unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.9(a)(6):</b>	Describe how the organization will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality	Described in the provided Data Security and Privacy policy

	and integrity of personally identifiable information in its custody.	
<b>NYCRR - 121.9(a) (7):</b>	Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.9(a) (8):</b>	Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.	Affirm
<b>NYCRR - 121.9(a) (b):</b>	Describe how the organization will supervise its subcontractors to ensure that as subcontractors perform its contractual obligations, the subcontractor will conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.10 (a):</b>	Describe how the organization shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.	Described in the provided Data Security and Privacy policy
<b>NYCRR - 121.10(f) :</b>	Affirmatively state that where a breach or unauthorized release is attributed to the organization, the organization shall pay for or promptly reimburse the educational agency for the full cost of such notification.	Affirm
<b>NYCRR - 121.10 (f.2):</b>	Please identify the name of your insurance carrier and the amount of your policy coverage.	State Farm
<b>NYCRR - 121.10(c) :</b>	Affirmatively state that the organization will cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.	Affirm
<b>Acceptable Use Policy Agreement:</b>	Do you agree with the Capital Region BOCES <a href="http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=BU4QYA6B81BF">Acceptable Use Policy?</a> (Click here: <a href="http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=BU4QYA6B81BF">http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=BU4QYA6B81BF</a> )	I Agree
<b>Privacy Policy Agreement:</b>	Do you agree with the Capital Region BOCES <a href="http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=BWZSQ273BA12">Privacy Policy?</a> (Click here: <a href="http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=BWZSQ273BA12">http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&amp;id=BWZSQ273BA12</a> )	I Agree
<b>Parent Bill of Rights:</b>	Please upload a signed copy of the Capital Region BOCES Parent Bill of Rights. A copy of the Bill of Rights can be found here: <a href="https://www.capitalregionboces.org/wp-content/uploads/2021/03/CRB_Parents_Bill_Of_Rights_-Vendors.pdf">https://www.capitalregionboces.org/wp-content/uploads/2021/03/CRB_Parents_Bill_Of_Rights_-Vendors.pdf</a>	CRB_Parents_Bill_Of_Rights_-Vendors-Press4Kids.pdf
<b>DPA Affirmation:</b>	By submitting responses to this Data Privacy Agreement the Contractor agrees to be bound by the terms of this data privacy agreement.	I Agree

### Attachments

Name	Size	Type	Upload Date	Downloads
No Records Found				

### Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

### Vendor Portal Details

<b>Contact Name:</b>	The Risk Mitigation & Compliance Office	<b>Publish Date:</b>	
<b>Required Portal Fields Populated:</b>	Yes	<b>Contact Email Address:</b>	crbcontractsoffice@neric.org
<b>About NYCRR Part 121:</b>	In order for a vendor to engage with a New York State Educational Agency, the vendor must provide information required by the New York State Commissioner's Regulations Part 121 (NYCRR Part 121) and the National Institute of Standards and Technology Cyber Security Framework. If deemed appropriate, the responses you provide will be used as part of the data privacy agreement between the vendor and the Albany-Schoharie-Schenectady-Saratoga BOCES. This Data Privacy Agreement	<b>Requesting Company:</b>	Capital Region BOCES

("DPA") is by and between the Albany-Schoharie-Schenectady-Saratoga BOCES ("EA"), an Educational Agency, and Press4Kids Inc. - News-O-Matic ("CONTRACTOR"), collectively, the "Parties". 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.

**Created By:**

**Third Party  
Name:**

Press4Kids Inc. - News-O-Matic

**Name:**

Press4Kids Inc. - News-O-Matic-279685

**Legacy Submit**

**Date:**