

# Cattaraugus-Allegany-Erie-Wyoming BOCES ("CA BOCES")

## DATA PRIVACY AGREEMENT

"utilizing New York State Model Data Privacy Agreement for Educational Agencies."

CA BOCES

---

and

ReadWorks

---

This Data Privacy Agreement ("DPA") is by and between the CA BOCES ("EA"), an Educational Agency, and ReadWorks ("Contractor"), collectively, the "Parties".

### ARTICLE I: DEFINITIONS

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

- 1. Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- 2. Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- 3. Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- 4. Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- 5. Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- 6. Eligible Student:** A student who is eighteen years of age or older.
- 7. Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or

indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 9. Parent:** A parent, legal guardian, or person in parental relation to the Student.
- 10. Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g, and Teacher or Principal APPR Data, as defined below.
- 11. Release:** Shall have the same meaning as Disclose.
- 12. School:** Any public elementary or secondary school including a charter school, universal 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.

## ARTICLE II: PRIVACY AND SECURITY OF PII

### 1. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated 10/01/22 ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with

Disabilities Education Act (“IDEA”) at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education’s Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

**2. Authorized Use.**

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

**3. Data Security and Privacy Plan.**

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA’s policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor’s Data Security and Privacy Plan is attached to this DPA as Exhibit C.

**4. EA’s Data Security and Privacy Policy**

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

**5. Right of Review and Audit.**

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

**6. Contractor’s Employees and Subcontractors.**

- (a) Contractor shall only disclose PII to Contractor’s employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is

contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.
- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

## **7. Training.**

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

## **8. Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

## **9. Data Return and Destruction of Data.**

- (a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable,

read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

#### **10. Commercial or Marketing Use Prohibition.**

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

#### **11. Encryption.**

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

#### **12. Breach.**

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

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

CA BOCES Data Privacy Officer  
1825 Windfall Road  
Olean, New York 14760  
[DPO@caboces.org](mailto:DPO@caboces.org)

#### **13. Cooperation with Investigations.**

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

be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

**14. Notification to Individuals.**

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

**15. Termination.**

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

### ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

**1. Parent and Eligible Student Access.**

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

**2. Bill of Rights for Data Privacy and Security.**

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

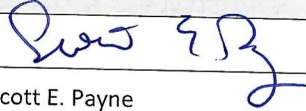
### ARTICLE IV: MISCELLANEOUS

**1. Priority of Agreements and Precedence.**

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

## 2. Execution.

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


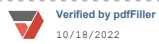
EDUCATIONAL AGENCY	
Signature:	
Printed Name:	Scott E. Payne
Title:	CA BOCES District Superintendent and Chief Executive Officer
Date:	10/20/2022

CONTRACTOR	
Signature:	 
Printed Name:	Caitlyn Meagher
Title:	Privacy Specialist
Date:	10/01/2022

## EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://www.nysed.gov/data-privacy-security/student-data-inventory) and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed.  
(i) Complaints should be submitted to the EA at: CA BOCES Data Privacy Officer, 1825 Windfall Road, Olean, New York 14760, via email at [DPO@caboces.org](mailto:DPO@caboces.org) or by using the form available at the following website: <https://caboces.org/resources/new-york-state-education-law-2d/report-an-improper-disclosure/>.  
(ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://www.nysed.gov/data-privacy-security/report-improper-disclosure), by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to [privacy@nysed.gov](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
Signature:	 
Printed Name:	Caitlyn Meagher
Title:	Privacy Specialist
Date:	10/01/2022




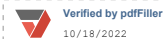
## EXHIBIT B

### BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY - SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

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

<b>Name of Contractor</b>	ReadWorks
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	All data is stored exclusively for educational purposes, either to ensure the smooth functionality of the website itself, or to support analysis in the aim of improving the ReadWorks product. No student PII is utilized for commercial or marketing purposes.
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date <u>10/18/2022</u> Contract End Date <u>09/31/2025</u>
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.</li> <li>Securely delete and destroy data.</li> </ul>
<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

<b>Secure Storage and Data Security</b>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: All subcontractors are upheld to the same standards of care explicated in ReadWorks' privacy policy.</p>
<b>Encryption</b>	<p>Data will be encrypted while in motion and at rest.</p>

<b>CONTRACTOR</b>	
<b>Signature:</b>	 
<b>Printed Name:</b>	<p>Caitlyn Meagher</p>
<b>Title:</b>	<p>Privacy Specialist</p>
<b>Date:</b>	<p>10/18/2022</p>

## EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

### CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	<a href="http://www.readworks.org/privacy">www.readworks.org/privacy</a>
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	ReadWorks stores and processes student data in accordance with industry best practices. This includes appropriate administrative, physical, and technical safeguards including firewalls to secure Student Data from unauthorized access, disclosure, and use. We conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. We regularly perform system audits and work to ensure all of our software has the latest security-related patches and updates.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	ReadWorks employees undergo an annual risk assessment to measure personal and company-wide security risks. Employees take steps to remedy any issues that arise.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	All subcontractors are upheld to the same standards of care explicated in ReadWorks' privacy policy.  ReadWorks has designated a Privacy Officer to monitor and oversee data policies and procedures. They will monitor cybersecurity threats, vulnerabilities and legal updates regularly as well as update software to provide further security. This Privacy Officer will also train employees regarding ReadWorks' procedures and policies surrounding data confidentiality. They will ensure trained employees only have access to sensitive data when necessary. In the first 24 hours after discovering any signs of a data breach, the Privacy Team will alert and activate everyone at ReadWorks. The team will ensure the area where the data breach occurred is secure to help preserve evidence and stop additional data loss. The Privacy Team will document who discovered the breach, who reported it and what type of breach occurred. They will interview all involved parties and document the results. With this information, they will ascertain what data has been compromised and what parties are affected by the breach. ReadWorks employees will then prepare external communications regarding the incident to reach out to the exposed parties in accordance with applicable laws and regulations. After a breach, trained employees, along with the Privacy Officer, will fix all issues that led to the incident in order to prevent further unauthorized access. They will also preserve any relevant evidence regarding the situation to further investigate and analyze the cause of said data breach.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	N/A
7	Describe your secure destruction practices and how certification will be provided to the EA.	N/A
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	<a href="http://www.readworks.org/privacy">www.readworks.org/privacy</a>
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

## EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies ); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional

Function	Category	Contractor Response
IDENTIFY (ID)	<b>Asset Management (ID.AM):</b> The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	
	<b>Business Environment (ID.BE):</b> The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	
	<b>Governance (ID.GV):</b> The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	
	<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	<b>Risk Management Strategy (ID.RM):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	
	<b>Supply Chain Risk Management (ID.SC):</b> The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	<b>Identity Management, Authentication and Access Control (PR.AC):</b> Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	

Function	Category	Contractor Response
	<b>Awareness and Training (PR.AT):</b> The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	
	<b>Data Security (PR.DS):</b> Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	
	<b>Information Protection Processes and Procedures (PR.IP):</b> Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	
	<b>Protective Technology (PR.PT):</b> Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	
DETECT (DE)	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	
	<b>Security Continuous Monitoring (DE.CM):</b> The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	
RESPOND (RS)	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	

Function	Category	Contractor Response
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	
RECOVER (RC)	<b>Recovery Planning (RC.RP):</b> Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	
	<b>Communications (RC.CO):</b> Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	

# Privacy Policy

---

*Last Updated: March 21, 2022*

Welcome! Thank you for visiting the ReadWorks, Inc. website (“ReadWorks”, “we”, “our”, or “us”). This Privacy Policy applies to our entire Site, including this website (readworks.org) and all of our subdomains (the “Site”).



When you visit our Site, you agree to our Privacy Policy and . In the case of any material changes to our policy, we will provide a banner notification on our website to inform all users of said changes. This notification will include an "accept" button on the banner. Once you have consented to these changes by clicking on the "accept" button, you can continue to use our Site. We encourage you to review this Privacy Policy now and each time you visit our Site. If you do not agree to any term in the Privacy Policy, you should not use the Site.

We are strongly committed to protecting the privacy of everyone who visits our Site, including our educator users and their students. This Privacy Policy should help you understand what information we collect about you and/or your students when you visit and use the Site and how we use any information we may collect. Before we get into the details, we want to say first and foremost that we are fully committed to student data privacy as we help educators improve student reading achievement.

If you have any questions, comments, or concerns about our Privacy Policy, please email us at or write to us at P.O. Box 24673, Brooklyn, NY 11202.

## **1. Children’s Privacy**

ReadWorks knows how important it is to protect children’s privacy. Our Site is intended for any U.S.-based adult educator or education-minded parent or guardian to use in concert with students of elementary school age or older. No student of any age is meant to use the ReadWorks Site without the invitation, direction, and guidance of an adult.

When educators, parents, or guardians create accounts on behalf of their students, we keep whatever name is provided by that adult in our database. When a student account in ReadWorks is set up from a pre-existing Google account, we collect the name provided by such educator, parent, or guardian as it appears in that Google account and store it in our database accordingly. With respect to any student accounts, we do not collect or store any student email addresses, including when a student uses a Google account to log in to the Site.

Collection or use of data is limited to product requirements. ReadWorks does not collect geolocation data, biometric or health data, or behavioral data. We collect student names to ensure that parents, guardians, and educators are able to keep track of which students are which while using our Site. We do not store student names long-term and endeavor to delete such data once the corresponding student account or the class containing such student account is deleted by the educator, parent or guardian who set up such account. Student use activity (e.g., when an assignment begins or ends and how questions are answered) is stored anonymously and retained only for educational purposes. ReadWorks will not retain student personal information for longer than necessary to deliver services or for school purposes. ReadWorks will delete any student data once operationally practicable. Users cannot interact with untrusted users, including strangers. ReadWorks' profile information is not shared for social interactions.

If you are the parent, guardian, or educator of a child who has used the Site without such permission, please contact us at .

## **2. How We Handle Data**

### **a. Information We Collect**

When you visit and use our Site, we may collect information about you.

- *Information you provide to us:* In order to get access to certain information or materials that are provided through the Site, you may have to provide information to us. We collect and store this information in a way that allows us to connect it to you personally, including, for example, your name and email address. We refer to this information as personal information. Additionally, we may collect and retain a record of all communications we have with you.



- *Information we collect through technology:* We may also collect information about you through technology. For example, we may collect your IP address each time you click on a page during a visit to our Site. The Site may also use other technical methods to track and analyze website traffic patterns, such as how often our users visit different parts of the Site. These technical methods may involve the transmission of information either directly to us or to another party we have authorized to collect and process information on our behalf, such as Amazon Web Services. More information on how Amazon Web Services uses data can be found at [https://aws.amazon.com/privacy/](#). We may also use technical methods in emails that we send educator or parent Site users to figure out if users have opened those emails and/or clicked on links in those emails. We may collect the information from these technical methods in a form that is personally identifiable.

## **b. Use of Collected Information**

We do not disclose nonpublic personal information about users of the Site to any nonaffiliated third parties, except as described here or in our Terms of Use.

We may use or disclose certain personal information we collect about our users when they visit and browse our Site as part of our normal operations, including through our promotional email platform, ActiveCampaign. We make every effort to segregate student data from that of educators, parents, and guardian users and do not share such data with ActiveCampaign. More information on how ActiveCampaign uses data can be found at [https://www.activecampaign.com/privacy-policy](#). We may also use or disclose certain personal information to respond to specific requests we get from you and through our use of service providers in connection with the Site. These third-party service providers may have access to and use your personal information, but only as needed to perform the functions we have asked them to perform. All third parties adhere to the same security and data retention principles as ReadWorks. ReadWorks only shares your personal information with third-party service providers that are consistent with our privacy policy.

ReadWorks does not display any advertisements on our Site nor provide promotional sweepstakes or contests. There is no traditional, contextual, or behavioral advertising on the ReadWorks website. Users can opt out or unsubscribe from marketing

communications by selecting the “Unsubscribe” button at the bottom of every email or emailing ReadWorks at [help@readworks.org](mailto:help@readworks.org).

When we believe we have to disclose something because it is required by law, regulation, legal process, subpoena, document, or governmental request, we will disclose personal information we collect from you. We may also do so to help enforce our Terms of Use, protect your safety or security, or protect the safety and security of tangible or intangible property that belongs to us, to you, or to third parties. We may transfer all user information (which may include personal information) to our acquirers or successors. Our acquirers and successors in the future will act in accordance with this privacy policy. Other than as part of such a transaction, we will not sell any of your personal information.

Non-personal information is information that does not personally identify you, including anonymous information and aggregate data. We may use this information to understand better how our visitors use the Site, provide visitors with customized services and information, improve the Site, and for other similar purposes. We may combine this information with personal information. We may share this information with others and use this information in any manner permitted by law, but any disclosure that identifies you personally will be governed by the above paragraphs on personal information.

### **3. Cookies**

Our Site uses “cookies” to enable ongoing access to and use of the Site and to help us in ongoing Site maintenance. Cookies are small text files that may be placed on a browser when you visit a web site. For instance, when you return to the Site after logging in, cookies provide information to the Site, including personal information, so that the Site can remember who you are.

We use cookies to capture anonymous data from the actions of our users to improve our Site experience and the way it performs. Our system is set up to not use cookies with our student users except in cases where it is requested by such student’s school district. In such cases, the data generated is managed by the school district’s privacy policy.

We get statistical information from cookies on, among other things, how often users use our Site, the pages users visit, and how long each visit is, as well as information about a user's computer, operating system, browser, language, and country. If you go to the settings on your Internet browser, you can choose to have your computer warn you each time a cookie is sent or you can choose to turn off all cookies. Check your browser's HELP menu to learn about your options. If you decide to turn off cookies, you may not have access to many features that make the use of our Site smoother, and some of the services on the Site might not work properly. You can delete any cookies at any time by using the relevant option of your Internet browser or by deleting cookies on your hard drive. If you continue to use the Site with your browser set to accept cookies, we will assume that you accept receiving all cookies coming from our Site.

#### **4. Google Analytics**

We use Google Analytics to collect information about how our visitors use our Site. Google Analytics collects information such as how often users visit the Site, what pages users visit, and what other sites they visited before or after coming to the Site. Our Site is set up to not use Google Analytics to collect data about our student users. More information on how Google Analytics uses data can be found at [. We use the information we get from Google Analytics only to improve our Site. By using our Site with your Internet browser set to accept cookies, you agree to Google Analytics' use of cookies on our Site.](#)

#### **5. Third Party Websites**

Our Site contains links to websites owned and operated by third parties. We provide these links for convenience, we do not have control over the content of these websites, and we do not take on any liability or responsibility for these sites. Our Privacy Policy does not concern the use of information collected on these third party sites. If you choose to visit these third party sites, you should review their privacy policies to make sure you understand and are comfortable with their practices regarding your personal information.

#### **6. Protection of Information**

We work hard to protect your personal information. We store and process student data in accordance with industry best practices. This includes encryption and appropriate administrative, physical, and technical safeguards including firewalls to secure Student Data from unauthorized access, disclosure, and use. We conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. We regularly perform system audits and work to ensure all of our software has the latest security-related patches and updates. We also limit employee access to user information. Unfortunately, there is no such thing as “perfect security” on the Internet, and third parties may unlawfully intercept or access transmissions or private communications. We will not be responsible or liable for any damages, losses, or causes of action in connection with the disclosure of your personal information.

## **7. Do Not Track**

We may track users’ use of the Site over time to continually improve our service to our users and our overall Site. Our Site is set up to not track student users’ use of the Site over time. We do not track visitors of the Site over time and across third party websites to provide targeted advertising and therefore do not respond to Do Not Track (“DNT”) signals. However, some third-party sites do keep track of browsing activity when they provide content, which allows them to tailor what they present to you. If you are visiting these sites, your browser allows you to set the DNT signal so that third parties (particularly advertisers) know you do not want to be tracked. You can consult the help pages of your browser to learn how to set your preferences so that websites do not track you.

## **8. Information Requests**

If you would like us to disclose to you or delete certain information about our collection and use of your personal information, you may ask us to do so. Once we receive your request and verify your identity, we will disclose such information to you or delete the information you have asked us to delete, unless there is a legal exception. For example, we might deny your deletion request if we have to keep the information in order for us or our providers to complete the transaction for which we collected the personal information, provide a service that you requested, or take actions we reasonably anticipate within the context of our ongoing relationship with you.

To submit a request please email us at .

Your request must:

- Provide enough information to allow us to reasonably verify that you are the person about whom we collected personal information or an authorized representative of such person.
- Describe your request with enough detail to allow us to understand, evaluate, and respond to it.

We cannot respond to your request or provide you with non-public personal information if we cannot verify your identity or authority to make the request and confirm that the requested personal information relates to you. We will use the information provided in a request solely to verify your identity or authority to make the request.

## **9. Shine the Light**

California Civil Code Section 1798.83, known as the “Shine The Light” law, permits our Site users who are California residents to request and obtain from us a list of their personal information (if any) we disclosed to third parties for direct marketing purposes in the preceding calendar year and the names and addresses of those third parties. Requests may be made only once a year and are free of charge. We currently do not share any personal information with third parties for their direct marketing purposes.

## **10. International Use**

This Site is intended for use by individuals in the United States. Despite the global nature of the Internet, ReadWorks makes no claims that the Site is appropriate or may be viewed or used outside the United States. Additionally, our databases are located in the United States, and the data we collect from users is stored in the United States. This Site is intended for use by individuals in the United States. ***By sending us your information, you consent to its transfer to and storage within the United States and its use in a manner consistent with this Privacy Policy.***

## **11. Governing Law**

The laws of the State of New York govern this Privacy Policy. Any dispute relating to this Privacy Policy or your use of the Site or the Content shall be resolved solely in the state or federal courts located in New York, New York.

## **12. Contact Us**

If you have any questions or comments about this Privacy Policy, you can email us at or write to us at P.O. Box 24673, Brooklyn, NY 11202.

Link to .