

## NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

**JAMESTOWN CITY SCHOOL DISTRICT**

**and**

**AMERICAN READING COMPANY**

---

This Data Privacy Agreement ("DPA") is by and between the Jamestown City School District ("EA"), an Educational Agency, and AMERICAN READING COMPANY ("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 \_\_\_\_\_ ("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:

Chief Information Officer  
Jamestown City School District  
197 Martin Road  
Jamestown NY 14701  
DPO@jpsny.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.


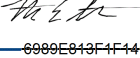
**ARTICLE IV: MISCELLANEOUS**

**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.

<b>EDUCATIONAL AGENCY</b>	<b>CONTRACTOR</b>
BY: 	BY:  <small>DocuSigned by:</small>
Name: <b>Jessie Joy</b>	Name: <b>Nathan Smith</b>
Title: <b>Chief Information Officer</b>	Title: <b>CTO</b>
Date: 11/7/22	Date: 11/4/2022



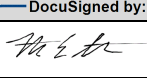
## EXHIBIT A

### Education Law §2-d Bill of Rights for Data Privacy and Security Jamestown City School District

The Jamestown City School District is committed to protecting the privacy of student data and teacher and principal data. In accordance with New York Education Law §2-d and its implementing regulations. 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.** Parents have 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.** Parents have the right to have complaints about possible breaches and unauthorized disclosures of PII addressed. Complaints should be submitted in writing to the Jamestown City School District, Data Protection Officer, 197 Martin Road, Jamestown NY 14701, or by email to [DPO@jpsny.org](mailto:DPO@jpsny.org). 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.** Parents will 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]	 DocuSigned by: 6989E813F1F14C9...
[Printed Name]	Nathan Smith
[Title]	CTO
Date:	11/4/2022


## 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>	American Reading Company
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	Please see attached security and privacy information
<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 _____ Contract End Date <u>6/30/23</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.

<p><b>Secure Storage and Data Security</b></p>	<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:</p> <p style="text-align: center;">Please see ARC's Digital Products Security and Privacy Policy attached.</p>
<p><b>Encryption</b></p>	<p>Data will be encrypted while in motion and at rest.</p>

<p><b>CONTRACTOR</b></p>	
<p>[Signature]</p>	<p>DocuSigned by:  </p>
<p>[Printed Name]</p>	<p>6989E813F1F14C9...  <b>Nathan Smith</b></p>
<p>[Title]</p>	<p><b>CTO</b></p>
<p>Date:</p>	<p>11/4/2022</p>

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

### CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

Pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations, the EA is required to ensure that all contracts with a third-party contractor include the contractor's Data Security and Privacy Plan. **The Contractor must complete the following or provide a plan that materially addresses these requirements.**

In addition to complying with the terms of the EA's Parents' Bill of Rights, Contractor shall protect the confidentiality, privacy and security of Protected Data received from the EA as set forth below:

1. In order to implement all state, federal, and local data security and privacy requirements, including those contained within this Data Privacy Agreement, and in a manner consistent with the EA's data security and privacy policy, Vendor shall take the following measures to implement all state, federal, and local data security and privacy requirements over the life of the agreement:

The attached documents titled, "ARC Digital Products- Security and Privacy" and "ARC New York Ed Law 2-d" outline how ARC will implement applicable data security and privacy contract requirements.

2. Contractor shall have the following administrative, operational and technical safeguards and practices in place to protect Protected Data that it receives from the EA under this Data Privacy Agreement:

Please see ARC's Digital Products Security and Privacy Policy attached.

3. Contractor shall comply with all of its obligations set forth in Appendix B, "Supplemental Information for Contracts that Utilize Personally Identifiable Information."

4. Contractor has provided or shall provide training on the federal and state laws governing confidentiality of Protected Data for any of its officers or employees (or officers or employees of any of its assignees, if any) who will have access to Protected Data, prior to their receiving access as follows:

All American Reading Company employees who are granted access to student data are trained in the safe-handling of student records. Among other provisions, employees are trained to never send or request student information via email or other insecure messaging solutions, never store exported student records on laptops, desktops, or mobile devices at any time.

5. Contractor  intends  does not intend to utilize subcontractors, assignees or other authorized agents for the purpose of fulfilling one or more of its obligations under this Data Privacy Agreement. In the event that Contractor engages any subcontractors to perform its obligations under this Data Privacy Agreement, it shall ensure such subcontractors abide by the data protection and security requirements contained in this this Data Privacy Agreement and applicable state and federal law by methods as more fully described in Appendix B, "Supplemental Information for Contracts that Utilize Personally Identifiable Information."

6. Contractor shall provide prompt notification to the EA of any breaches or other unauthorized disclosures of Protected Data in accordance with the provisions of Section 5 of this Data Privacy Agreement. Contractor shall manage data security and privacy incidents that implicate Protected Data, including plans to identify breaches as follows:

Please see ARC's Digital Products Security and Privacy Policy attached.

7. Contractor shall implement the procedures for the return, transition, deletion and/or destruction of Protected Data at such time that this Data Privacy Agreement expires or is terminated as more fully described in Appendix B, "Supplemental Information for Contracts that Utilize Personally Identifiable Information."

# ARC Digital Products

## Security and Privacy

### Security and Disaster Recovery

ARC digital products adhere to the following security and disaster recovery practices:

- All web-based services and RESTful API calls use TLS 1.2 security.
- All personally identifiable information stored in MySQL is encrypted at rest using InnoDB tablespace encryption.
- ARC digital products offer access for teachers, school administrators, and district administrators as identified by the district. Users in each of those security groups have access to only those student records in their scope of responsibility.
- For districts using Clever Instant Login or Classlink OneClick Single Sign-On, the district maintains real-time control of all user credentials. For districts not using one of our supported single sign-on solutions, districts may assign usernames and passwords up to 128 characters. All passwords are stored using BCrypt encryption.
- The TrueNet data center includes biometric door locks coupled with NFC cards. All server cabinets are locked.
- Servers at the TrueNet data center have dual power supplies connected to separate power circuits with battery backup.
- All data at the TrueNet data center is stored on striped and mirrored hard drives for redundancy.
- All digital product data is replicated to multiple database servers behind our firewalls.
- All data is backed up daily using Dell RapidRecovery, encrypted, and transferred securely to ARC's headquarters.
- All employees who might require access to secure data are provided with training in safe-handling procedures.

## Cloud Hosting

ARC digital products are hosted on the Microsoft Azure cloud platform. Through the use of encryption and restricted access to physical devices, Microsoft does not have access to district data in any form at any time.

- One Microsoft Way, Redmond, WA, 98052
- (800) 426-9400
- Security Information for the Microsoft Azure platform, including attestations for NIST, SOC2, and other compliance offerings, can be found here:  
<https://learn.microsoft.com/en-us/azure/compliance/offerings/>

## Privacy

- Data stored in ARC digital products remains the property of the district and is protected by several policies to ensure privacy.
- American Reading Company does not share district data with any third parties unless requested by district administration.
- **FERPA Compliance:** American Reading Company's software products meet the requirements of FERPA. Acting as a school official with legitimate educational interests, American Reading Company receives basic directory information from the district in order to populate ARC digital products with student rosters. To facilitate information review by parents, legal guardians, and eligible pupils, ARC digital products include several printable reports, including the Student History Report and Status of the Class, that may be printed by district staff. If erroneous information is found in student records, parents, legal guardians, and eligible pupils may contact the district to request a modification of the erroneous records. For districts using an automated rostering solution, the incorrect student records will need to be modified in the root SIS system. Changes will be synchronized to American Reading Company's software platform within 24 hours. For districts not using an automated rostering solution, district personnel may make corrections to student records directly in American Reading Company's software platforms.
- **COPPA Compliance:** American Reading Company's software products meet the requirements of COPPA. All of American Reading Company's software products are marketed and sold to schools and districts, not directly to students. No personal data is collected from students, and students are never prompted to enter any personal information. Any rostering and demographic data used to populate class lists and other constructs is entered by authorized district or school personnel.
- **CIPA Compliance:** American Reading Company's software products meet the requirements of CIPA. At the time of this writing, American Reading Company offers three software products, SchoolPace Connect, ARC Bookshelf and ARC



Adventures, that are used directly by students. These products do not offer open or unfiltered access to Internet resources. Rather, they are curated collections of curricular resources, digital books, and foundational skills practice activities, respectively. This content has been vetted for age appropriateness.

- **GDPR Compliance:** American Reading Company's software products meet the "Lawfulness of Processing" requirement of the General Data Protection Regulation (GDPR) based on Chapter 2, Article 6, Section 1.b.: *"processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;"* <https://gdpr.eu/article-6-how-to-process-personal-data-legally/> In addition, American Reading Company's cloud provider, Microsoft Azure, fully complies with GDPR, as described in the following document: <https://docs.microsoft.com/en-us/legal/gdpr>
- All American Reading Company employees who are granted access to student data are trained in the safe handling of student records. Among other provisions, employees are trained to never send or request student information via email or other insecure messaging solutions, never share access, and never store exported student records on laptops, desktops, or mobile devices at any time.

## Handling of Breaches, Data Privacy Incidents, and Security Incidents

- **Cyber Security Insurance:** American Reading Company is protected by a cyber security policy provided by CNA. The individual event and aggregate coverage limits for this policy are both \$5,000,000.
- **Audit Logs:** ARC digital products collect a variety of audit logs of user activity. Logs are retained until the end of the agreement term with each customer. These logs include, but are not limited to, the following activities:
  - For every user log in, the user identifier, IP address, and timestamp are recorded.
  - Each insert, update, and deletion of data is logged with a user identifier and timestamp.
  - The viewing of documents, digital books, and videos is logged with a user identifier and timestamp.
  - The exporting of artifacts including PDF files, CSV files, and Excel files is logged with a user identifier and timestamp.
- **Error Logs and Access Logs:** All system logs, including error logs and server access logs, are captured, and aggregated on a third-party log aggregator, NewRelic.
- **Intrusion Detection and Prevention:** ARC digital products are hosted behind redundant SonicWall network security appliances. These appliances apply the following intrusion detection and prevention safeguards:
  - Firewall with Deep Packet Inspection (DPI)
  - SonicWall Intrusion Prevention Service (IPS)
- **Notification:** Upon detection of a data breach, American Reading Company will send an email and place a phone call to the designated security contact for the affected school district within 24 hours. If no security contact is specified, American Reading Company will notify the district's IT department. Notifications will include:
  - The nature of the breach.
  - The number of PII records affected.
  - A description of how the breach was identified.

## Data Sharing

American Reading Company receives basic directory information from the district to populate our digital products with student rosters. This rostering data is used to create schools, classrooms, and student records in our databases. This basic rostering data is necessary to allow teachers and administrators to collect reading performance data, view reports based on this data, and provide access to appropriate resources and content. The following data is collected:

Students		Teachers and Administrators	
<ul style="list-style-type: none"> <li>• Student Identification Number</li> <li>• Prefix *</li> <li>• First Name</li> <li>• Middle Name *</li> <li>• Last Name</li> <li>• Suffix *</li> </ul>	<ul style="list-style-type: none"> <li>• Gender *</li> <li>• Ethnicity *</li> <li>• Date of Birth *</li> <li>• Grade</li> <li>• Classroom Assignments</li> </ul>	<ul style="list-style-type: none"> <li>• Prefix *</li> <li>• First Name</li> <li>• Middle Name *</li> <li>• Last Name</li> <li>• Suffix *</li> </ul>	<ul style="list-style-type: none"> <li>• Email Address</li> <li>• Security Level (Teacher, School Administrator, District Administrator)</li> <li>• Classroom Assignments</li> </ul>
<p><i>Items marked with an asterisk (*) are optional.</i></p>			

ARC is committed to using data to improve student outcomes. To this end, ARC will report aggregate, anonymized data as part of research and evaluation efforts, and other efforts related to improving the implementation of ARC products and services. ARC will report aggregate, anonymized data to enable districts to examine how student performance in their district compares with other districts. ARC may report aggregate system-wide, district-level, subgroup-level, grade-level, and school-level data. No district, school, teacher, or student will ever be named. For example, ARC may report that the average IRLA reading level for all 3<sup>rd</sup> graders, system-wide, is 2.79.

## Other Data Sharing Agreements

When ARC and a district agree to use SchoolPace data and/or other district data for research purposes, a separate data sharing agreement is put into place. The research DSA documents the terms under which the District will share data from students' education records, including personally identifiable information (PII), with ARC in a manner consistent with FERPA and its implementing regulations, and district privacy policies.

# American Reading Company

## Compliance with Supplemental Information Regarding Third-Party Contractors

### New York State Ed Law 2-D

For purposes of further ensuring confidentiality and security of student data, as an appendix to the Parents' Bill of Rights each contract an educational agency enters into with a third party contractor shall include the following supplemental information:

American Reading Company's digital products, including SchoolPace, SchoolPace Connect, ARC Bookshelf, and ARC Adventures, comply with New York State Ed Law 2-d.

1. The exclusive purposes for which the student data, or teacher or principal data, will be used;
  - a. SchoolPace
    - i. Teachers use SchoolPace to assess student progress. While conferencing with students, teachers record observations about student learning. Teachers have access to charts, graphs, and other reports that aggregate student progress data for the students in their classrooms.
    - ii. School administrators use SchoolPace to monitor the progress of students, classrooms, and student groups within their school.
    - iii. District administrators use SchoolPace to monitor the progress of students, classrooms, student groups, and schools within their district.
    - iv. American Reading Company's team of professional developers use SchoolPace to generate reports for the schools they service, in accordance with district contracts and data sharing agreements.
    - v. American Reading Company's technical support team uses SchoolPace to configure rosters, settings, and reports for the districts they service. In addition, the technical support team may access data to troubleshoot customer concerns.
    - vi. Students use SchoolPace to view their own progress and view coaching tips tailored to their current progress. No personally identifiable information (PII) is collected from students directly.
    - vii. Family members use SchoolPace to view the progress of their student(s) and view coaching tips tailored to the current progress of their student(s). No personally identifiable information (PII) is collected from family members directly.
  - b. SchoolPace Connect
    - i. Teachers, administrators, students, and families use SchoolPace Connect to access digital resources, lessons, and videos from American Reading Company. Rostering data is used to provide the correct content to each teacher and student. Analytics data tracks which users have accessed each resource, and how long each resource was used.
  - c. ARC Bookshelf
    - i. Teachers and students use ARC Bookshelf to access digital books. Rostering data is used to provision the correct books to each teacher and student. Analytics data tracks which users have accessed each digital book, how much time was spent on each page, and other data.
  - d. ARC Adventures



5. 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, including whether such data will be encrypted.
  - a. American Reading Company's digital products adhere to the following security and disaster recovery practices:
    - i. All web-based services and RESTful API calls use TLS 1.2 security.
    - ii. All personally identifiable information stored in MySQL is encrypted at rest using InnoDB tablespace encryption.
    - iii. ARC digital products offer access for teachers, school administrators, and district administrators as identified by the district. Users in each of those security groups have access to only those student records in their scope of responsibility.
    - iv. For districts using Clever Instant Login or Classlink OneClick Single Sign-On, the district maintains real-time control of all user credentials. For districts not using one of our supported single sign-on solutions, districts may assign usernames and passwords up to 128 characters. All passwords are stored using BCrypt encryption.
    - v. The TrueNet data center includes biometric door locks coupled with NFC cards. All server cabinets are locked.
    - vi. Servers at the TrueNet data center have dual power supplies connected to separate power circuits with battery backup.
    - vii. All data at the TrueNet data center is stored on striped and mirrored hard drives for redundancy.
    - viii. All digital product data is replicated to multiple database servers behind our firewalls.
    - ix. All data is backed up daily using Dell RapidRecovery, encrypted, and transferred securely to ARC's headquarters.
    - x. All employees who might require access to secure data are provided training on safe-handling procedures.