

Parents' Bill of Rights for Data Privacy and Security

The Rensselaer City School District is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with [New York Education Law Section 2-d](#) and its implementing regulations, the District informs the school community of the following:

- 1) A student's personally identifiable information cannot be sold or released for any commercial purposes.
- 2) Parents have the right to inspect and review the complete contents of their child's education record.
- 3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
- 4) A complete list of all student data elements collected by New York State is available for public review at the following website <http://www.nysed.gov/data-privacy-security/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.
- 5) Parents/guardians who believe there has been a possible breach of student data should direct their concerns/complaints to the District Data Protection Officer, David Howell, at 518-396-3490 or dhowell@rcsd.k12.ny.us.
- 6) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/common/nysed/files/programs/data-privacy-security/nysed-cpo-data-incident-reporting-form.pdf>.

APPENDIX

Supplemental Information Regarding Third-Party Contractors

In the course of complying with its obligations under the law and providing educational services to District residents, the Rensselaer City School District has entered into agreements with certain third-party contractors. Pursuant to these agreements, third-party contractors may have access to "student data" and/or "teacher or principal data," as those terms are defined by law and regulation.

For each contract or other written agreement that the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District, the following supplemental information will be included with this Bill of Rights:

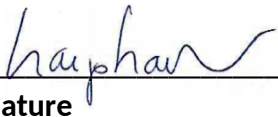
1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);
3. The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other

written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

4. If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;
5. Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and
6. Address how the data will be protected using encryption while in motion and at rest.
7. Third-party contractors are also required to:
 - a. Provide training on federal and state law governing confidentiality to any officers, employees, or assignees who have access to student data or teacher or principal data;
 - b. Limit internal access to education records to those individuals who have a legitimate educational interest in such records.
 - c. Not use educational records for any other purpose than those explicitly authorized in the contract;
 - d. Not disclose personally identifiable information to any other party without the prior written consent of the parent or eligible student; or (ii) unless required by statute or court order and the third-party contractor provides a notice of the disclosure to the New York State Education Department, board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order;
 - e. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable student information in its custody;
 - f. Use encryption technology to protect data while in motion or in its custody from unauthorized disclosure as specified in Education Law 2-d;
 - g. Notify Rensselaer City School District of any breach of security resulting in an unauthorized release of student data, in the most expedient way possible and without unreasonable delay;
 - h. Provide a data security and privacy plan outlining how all state, federal and local data security and privacy contract requirements will be implemented over the life of the contract;
 - i. Provide a signed copy of this Bill of Rights to the Rensselaer City School District thereby acknowledging that they are aware of and agree to abide by this Bill of Rights.

8) This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department Chief Privacy Officer, as well as emerging guidance documents.

BY Vendor:



Signature

CTO, LSD Software
Title

7/26/2021
Date

8 NYCRR Part 121	
121.2 Each educational agency shall ensure that it has provisions in its contracts with third party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with Federal and State law and the educational agency's data security and privacy policy.	RCSD Obligation
121.3(b) The bill of rights shall also be included with every contract an educational agency enters with a third-party contractor that receives personally identifiable information. The supplemental information must be developed by the educational agency and include the following Information:	RCSD Obligation
121.3(b)(1) What is the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?	Basic user profile data is collected solely for authentication purposes, to authorize users to access our services.
121.3(b)(2)/121.9(a)(b) Will the organization use subcontractors? If so, how will the organization ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., FERPA; Education Law section 2-d)?	No
121.3(b)(3) What is the duration of the contract including the contract's expected commencement and expiration date? Describe what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be destroyed). (page 1)	8/7/2021 to 8/7/2026 Unless the contract is renewed, the education agency may request all data related to the contract be deleted from our system.
121.3(b)(4) How can a parent, student, eligible student, teacher or principal challenge the accuracy of the student data or teacher or principal data that is collected?	Users can request to update their information either via our front-end web applications, or by emailing us at support@lsdsoftware.com
121.3(b)(5) Describe where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will	All collected user data are stored in our secure product database system hosted on AWS, behind application and network firewalls with strict access control. The DMBS is only accessible to

be protected and data security and privacy risks mitigated.	server applications and to server maintenance engineers.
121.6(a) Please submit the organization's data security and privacy plan that is accepted by the educational agency.	https://readaloud.app/privacy.html
121.6(a)(1) Describe how the organization will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;	LSD Software continually reviews and updates its security infrastructure to meet the highest standards and comply with federal, state, and local privacy requirements.
121.6(a)(2)/121.9(a)(6) Specify and describe the administrative, operational and technical safeguards and practices it has in place to protect the security, confidentiality and integrity of personally identifiable information in its custody that it will receive under the contract;	LSD Software takes disciplinary actions against violators of its security policies. We have stringent approval and audit processes for access to sensitive subsystems and data. Using industry standard Identity and Access Management software processes, we secure the data and grant only minimum access to application programs and to developers who need those data to do their jobs.
121.6(a)(4) Specify how officers or employees of the organization and its assignees who have access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access;	We issue company-wide notices to employees and officers with update-to-date instructions about how to comply with our privacy practices.
121.6(a)(5) Specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;	Subcontractors do not get access to real user data. All software development work will be done against mock data. So there is no risk to users' PII.
121.6(a)(6) Specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;	Incidents are reviewed by our administrators, and they will contact all affected parties via email or other means provided at the time of the signed contract.
121.6(a)(7) Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.	The education agency can request their data be returned, migrated, or deleted at any time by writing to us at support@lsdsoftware.com
121.9(a)(1) Describe the organization's adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework;	LSD Software observes the guidelines set out by the NIST Cybersecurity Framework. We have implemented strategies for identifying, protecting, detecting, responding, and recovering from cybersecurity events.
121.9(a)(2) Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts;	LSD Software collects only the minimal information required for the operation of its

<i>Education Law section 2-d</i> ; and this Part;	applications, and does not disclose this data to any third parties.
121.9(a)(3) Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;	Protected data is securely stored in our production servers only accessible to application software. Employees have no access unless authorized to perform server maintenance.
121.9(a)(4) Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract;	Use of PII data for any other purpose than that stated in our privacy policy is strictly prohibited by company policy.
121.9(a)(5) Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student; (i)except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with State and Federal law, regulations and its contract with the educational agency; or (ii)unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.	LSD Software's company policy does not permit the use of user PII data for any purpose other than the authentication for its software applications. (i) Subcontractors, if any, will not get access to real users' data; they will use mock data for all software development work. (ii) LSD Software complies with state and federal laws, and will promptly notify the educational institution should it be required to disclose user PII to government agencies.
121.3(b)(6)/121.9(a)(7) Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest; and	Data is sent to our server over HTTPS and secured by TLS. Data stored on the server is not encrypted.
121.9(a)(8) Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.	LSD Software does not sell user PII to third-parties
121.10(a) Describe how the organization shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.	We maintain all our signed contracts. Countersigned parties will be notified immediately of any privacy incidents via email.
121.10(c) Affirmatively state that the organization will cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.	We shall cooperate fully to protect the integrity of investigations into breach or unauthorized release of our users' PII.

121.10(f) Affirmatively state that where a breach or unauthorized release is attributed to the organization, the organization shall pay for or promptly reimburse the educational agency for the full cost of such notification.	LSD Software will reimburse the educational agency for any damage incurred by a breach attributed to us.
---	--