

## 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](mailto: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:

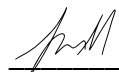
1. The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;
2. How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will 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 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**

\_\_\_\_\_  
**Chief Operating Officer**

**Title**

\_\_\_\_\_  
**8/6/2021**

**Date**

8 NYCRR Part 121	
<b>121.2</b> 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
<b>121.3(b)</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
<b>121.3(b)(1)</b> What is the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?	Free digital reading and writing lessons for grades 3-12, plus supplemental school and district resources, and research and development for the continued improvement of lessons and services
<b>121.3(b)(2)/121.9(a)(b)</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; <a href="#">Education Law section 2-d</a> )?	CommonLit uses subcontractors. All subcontractors are bound by written agreements to follow all relevant legal data privacy obligations and to protect PII no less strenuously than CommonLit does. In addition, CommonLit provides training on these obligations upon hire and in annual refresher trainings
<b>121.3(b)(3)</b> 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)	The contract will commence on 8/6/2021 and will terminate on 8/5/2026.  Upon expiration with no successor agreement CommonLit will delete all PII. CommonLit can also transfer a copy of the data to RCSD using SFTP if that is requested.
<b>121.3(b)(4)</b> How can a parent, student, eligible student, teacher or principal challenge the accuracy of the student data or teacher or principal data that is collected?	RCSD may contact us by sending an email to <a href="mailto:security@commonlit.org">security@commonlit.org</a> and then CommonLit will address any identified requests for review or updating
<b>121.3(b)(5)</b> Describe where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will	CommonLit uses Amazon Web Service's data centers in the continental United States to securely store assignment data, in compliance with industry standards including FERPA, COPPA, and FISMA. Data within our applications are

be protected and data security and privacy risks mitigated.	encapsulated in PostgreSQL, encrypted at rest, and require a secure SSL connection for access with internal services to protect sensitive personally identifiable information from unauthorized access. Separate services including RedShift are utilized for large scale warehousing and intensive data analytics.
<b>121.6(a)</b> Please submit the organization's data security and privacy plan that is accepted by the educational agency.	Our data privacy policy can be found at <a href="https://www.commonlit.org/en/privacy">https://www.commonlit.org/en/privacy</a> . In addition, we meet or exceed industry standards for data security and meet all federal, state, and contractual data obligations. Our platform also aligns with the NIST Cybersecurity framework, as illustrated by the form attached below this checklist.
<b>121.6(a)(1)</b> Describe how the organization will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy;	CommonLit complies with all federal, state, local, and contractually mandated data security and privacy rules, regulations, and requirements.
<b>121.6(a)(2)/121.9(a)(6)</b> 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;	CommonLit encrypts data at rest and in motion; administrative, operational, and technical best practices are followed; staff receive training on data security and privacy best practices training.
<b>121.6(a)(4)</b> Specify how officers or employees of the organization and its assignees who have access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access;	All employees and contractors receive training on all legally mandated data security requirements upon hire and they receive a yearly refresher training in the fall
<b>121.6(a)(5)</b> Specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;	CommonLit uses subcontractors. All subcontractors are bound by written agreements to follow all relevant legal data privacy obligations and to protect PII no less strenuously than CommonLit does. In addition, CommonLit provides training on these obligations upon hire and in annual refresher trainings
<b>121.6(a)(6)</b> Specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;	CommonLit maintains a plan to respond to any data security and privacy incidents that implicate PII, based on the details of the incident and the data implicated. CommonLit continuously monitors its site and database for breaches and works with third-party security consultants.
<b>121.6(a)(7)</b> Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the	Upon contract termination, or earlier at RCSD's request, CommonLit can securely delete all PII or provide copies to RCSD using SFTP.

educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.	
<b>121.9(a)(1)</b> Describe the organization's adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework;	Please see the attached chart
<b>121.9(a)(2)</b> Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts; <a href="#">Education Law section 2-d</a> ; and this Part;	CommonLit complies with all federal, state, local, and contractually mandated data security and privacy rules, regulations, and requirements. All employees and contractors receive training on these obligations
<b>121.9(a)(3)</b> Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;	Each employee or subcontractor only has permission to view PII and other data that pertains to their role, they do not have blanket access to all data held by CommonLit
<b>121.9(a)(4)</b> Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract;	All data is stored on secure servers and encrypted while in motion and at rest. Data is only available to those who have a need to access it. In addition, CommonLit only uses PII for the purposes allowed under contract
<b>121.9(a)(5)</b> Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student; <b>(i)</b> 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 <b>(ii)</b> 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.	CommonLit never releases PII to outside parties unless specifically requested by LEA or another party authorized under the contract. In the event that we are subject to a subpoena or other legal process that will mandate disclosure we will provide notice to RCSD unless the legal authority specifically prohibits such notice.
<b>121.3(b)(6)/121.9(a)(7)</b> Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest; and	We use industry standard encryption while data is in motion and at rest. Please see the attached chart for other information on how our policies align with the NIST Cybersecurity framework.
<b>121.9(a)(8)</b> Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.	CommonLit shall not sell PII nor use or disclose it for any marketing or commercial purpose. CommonLit will also not permit or enable another party to do so.
<b>121.10(a)</b> Describe how the organization shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of	In the event of a data breach CommonLit will notify RCSD's designated point of contact within

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.	7 calendar days of discovery. This notice will be provided through email.
<b>121.10(c)</b> Affirmatively state that the organization will cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.	CommonLit will cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII.
<b>121.10(f)</b> Affirmatively state that where a breach or unauthorized release is attributed to the organization, the organization shall pay for or promptly reimburse the educational agency for the full cost of such notification.	Where a breach or unauthorized release is attributed to CommonLit, CommonLit shall pay for or promptly reimburse RCSD for the full cost of such notification.

By:  \_\_\_\_\_

Agnes Malatinszky (Printed Name)

Chief Operating Officer (Title)

8/26/2021 (Date)

## NIST CSF TABLE

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	CommonLit has an organizational policy around locking computers and data storage, important accounts, and access to production level data and our code. User profiles with limited access to data as needed.

Function	Category	Contractor Response
	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.	CommonLit limits use and access to PII whenever possible. Use of the data is aligned to organization's mission, objectives, and stakeholders.
	<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.	CommonLit performs ongoing security audits of the application through a third party. We have individuals on staff trained on privacy requirements and regulations, and we work with external counsel as needed.
	<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.	CommonLit performs ongoing security audits of the application through a third party. We have individuals on staff trained on privacy requirements and regulations, and we work with external counsel as needed.
	<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.	Risk management and data access are evaluated for each individual who comes into contact with PII.
	<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.	CommonLit employs several tools that conduct ongoing analysis of ongoing software dependencies. Perform static analysis of application code and software dependencies in every build of software.
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.	Access to facilities is limited by physical security measures (locks, etc.) and virtual assets are tightly controlled by a limited policy that's limited to engineering and user support teams, with user support receiving less access than engineers. Credentials are regularly rotated, including upon termination or departure of any members with access.
	<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.	Staff receive training upon starting employment, and thereafter once a year phishing training, ongoing informal training, and data security and privacy training.
	<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.	We tightly limit access to raw data in general. In instances where people receive access to data, we consider whether partial or obfuscated data can be provided instead.

Function	Category	Contractor Response
	<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.	CommonLit maintains industry standard data security policies, processes, and procedures.
	<b>Maintenance (PR.MA):</b> Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	We perform regular ongoing maintenance of our application, infrastructure, and data, including finding anomalies, removing unused code and data.
	<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.	We perform regular ongoing penetration testing of the site.
<b>DETECT (DE)</b>	<b>Anomalies and Events (DE.AE):</b> Anomalous activity is detected and the potential impact of events is understood.	We perform some analysis for anomalous events including anomalous network traffic, data, and transactions.
	<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.	We perform regular ongoing third-party penetration testing of the site in addition to in-house monitoring by our engineering team.
	<b>Detection Processes (DE.DP):</b> Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Our team performs regular transfer anomaly testing.
<b>RESPOND (RS)</b>	<b>Response Planning (RS.RP):</b> Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	CommonLit has a data breach plan.
	<b>Communications (RS.CO):</b> Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Yes, response plans include coordination with internal and external stakeholders.
	<b>Analysis (RS.AN):</b> Analysis is conducted to ensure effective response and support recovery activities.	Plans include analysis to ensure effective response and support activities.
	<b>Mitigation (RS.MI):</b> Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Plan includes analysis to ensure effective response and support recovery activities.
	<b>Improvements (RS.IM):</b> Organizational response activities are improved by incorporating lessons learned from	Plans include organizational response activities to improve functions by incorporating lessons learned from current and

Function	Category	Contractor Response
	current and previous detection/response activities.	previous detection/response activities. We also conduct retrospectives and retro analysis.
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.	Recovery plan and process is available and maintained to ensure restoration of systems and assets affected by cybersecurity incidents.
	<b>Improvements (RC.IM):</b> Recovery planning and processes are improved by incorporating lessons learned into future activities.	We conduct retrospectives and retro analysis to improve processes 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).	Plans include restoration activity coordination with internal and external parties.