

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.

NYCRR - 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?

No student data is required to be entered for our hardware and software to provide the necessary solutions within K12. At the discretion of the school they may choose to enter student data or principal data - generally this would be a name and/or student ID.


NYCRR - 121.3 (b)(2):

Will the organization use subcontractors? If so, how will the organization ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., FERPA; Education Law section 2-d, NIST Cybersecurity Framework)?

We do not and will not use subcontractors to deliver any of our services.

NYCRR - 121.3 (b)(3):	What is the duration of the contract including the contract's expected commencement and expiration date? If no contract applies, describe how to terminate the service. Describe what will happen to the student data or teacher or principal data upon expiration. (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be securely destroyed and how all copies of the data that may have been provided to 3rd parties will be securely destroyed)	At present there is no contract in place. Should the end-user (school) utilize the Company's CLOUD service and at its discretion enter data which they wish to delete, the school has the ability to delete such data at any time.
NYCRR - 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?	The data that may entered at the discretion of a school would that of a student name and or ID. The school itself enters the data and can alter/modify the data at their discretion.
NYCRR - 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 be protected and data security and privacy risks mitigated.	Such data will be stored within the AWS CLOUD services environment, all of which is stored within the United States. Refer https://aws.amazon.com/compliance/ We employ role based security, where access control can be restricted based on what privileges are needed, allowed the adoption of least privilege practices. LockNCharge support and administrator access is limited to only those staff who require it, with access logged into an audit log.
NYCRR - 121.3 (b)(6):	Please describe how and where encryption is leveraged to protect sensitive data at rest and while in motion. Please confirm that all encryption algorithms are FIPS 140-2 compliant.	All data is encrypted at rest. All data is encrypted in transit, including within the internal sub systems. We use AWS Key Management Service (HSM) for encryption. HMS is FIPS-2 compliant.
NYCRR - 121.6 (a):	Please submit the organization's data security and privacy plan that is accepted by the educational agency.	Security and Compliance at LocknCharge.pdf
NYCRR - 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.	Compliance is as outlined in the uploaded document 121.6(a).
NYCRR - 121.6 (a)(2):	Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the engagement. If you use 3rd party assessments, please indicate what type of assessments are performed.	At LocknCharge, we take data integrity and security very seriously. Our facilities, processes and systems are reliable and robust. We continuously look for opportunities to make improvements and give you a highly secure, scalable system to provide a great experience to you. LocknCharge lets you deliver a secure system by: Securing your personal information: Compliance with Australia Privacy Act and GDPR. Ensuring Internal Data security of your data that rests with LocknCharge: Full data encryption in transit and at rest. Network Security: Automated locker hardware cannot expose your network to malicious activity from the Internet because it does not accept any inbound connections, such as SSH or telnet. The Cloud connection cannot expose you network to malicious activity from the Internet because the connection is always initiated from the hardware and is a simple messaging protocol secured using cryptographic certificates.
NYCRR - 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.	Employees will only have access to such data upon pre-approval from the school. Such employees will be informed of the relevant Federal and State laws governing such data.
NYCRR - 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.	Not applicable - We do not and will not use subcontractors to deliver any of our services.

<p>NYCRR - 121.6 (a)(6):</p>	<p>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.</p>	<p>We use both internal and multiple external monitoring services to monitor the LocknCharge Cloud Platform. Our monitoring system will alert the Operations & Security Team through emails and phone calls if there are any errors or abnormalities. Our employees are trained in how to communicate incidents internally and our customers are kept informed of incidents that affect their service. In cases that affect a small subset of our customers we may reach out directly to those affected customers.</p>
<p>NYCRR - 121.6 (a)(7):</p>	<p>Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires. Vendor will be required to complete a Data Destruction Affidavit upon termination of the engagement.</p>	<p>Customers can delete their account from the Cloud portal. This action triggers complete deletion of all customer data. Data is deleted within 60 days after an account is deleted.</p>
<p>NYCRR - 121.9 (a)(1):</p>	<p>Is your organization compliant with the NIST Cyber Security Framework?</p>	<p>No</p>
<p>NYCRR - 121.9 (a)(2):</p>	<p>Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law section 2-d; and this Part.</p>	<p>Compliance is as outlined in the uploaded agreement 121.6(a). When notified of any changes to the data security and privacy policy from BOCES we will review and reaffirm.</p>
<p>NYCRR - 121.9 (a)(3):</p>	<p>Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need authorized access to provide services.</p>	<p>We operate on a least privilege principle using role-based access control policy. LocknCharge, use two-factor authentication to grant access for our administrative operations to infrastructure. Administrative privileges are restricted to very few employees. Any administrative access is automatically logged. Detailed information on when/why the operations are carried out are documented and security considerations are taken into account before performing any changes in the production environment. Access reviews are conducted for standard users annually and privileged accounts every six months. All changes are logged and reviewed.</p>
<p>NYCRR - 121.9 (a)(4):</p>	<p>Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract. (e.g. Role Based Access, Continuous System Log Monitoring/Auditing)</p>	<p>Our ISMS systems are provided by cloud products and we are able to restrict access and log administrator level access via their tooling.</p>
<p>NYCRR - 121.9 (a)(5):</p>	<p>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.</p>	<p>We do not share or sell data to third parties.</p>
<p>NYCRR - 121.9 (a)(6):</p>	<p>Describe how the organization will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody.</p>	<p>Vulnerability Scanning & Patching: We periodically check and apply patches for third-party software/services. As and when vulnerabilities are discovered we apply the fixes. We do periodic vulnerability scanning using authorized services.</p>

<p>NYCRR - 121.9 (a)(7):</p>	<p>Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest.</p>	<p>Communication between LocknCharge hardware and the Cloud Platform: All communication between LocknCharge hardware and the Cloud Platform uses a secure IoT / MQTT channel - requires certificate signed by root CA which enables connection only under that device's unique identifier. It is impossible to access other devices or account data. Public HTTPS endpoint: endpoint discovery for single calls from device. API Gateway endpoints: OAuth token authenticated at the specific account level (no unauthenticated endpoints) Public API security is controlled through user-created app client identities. These are used by the client to fetch OAuth tokens, which in turn are used to authenticate API requests. App clients can be created by customers and revoked by customers or LocknCharge if necessary. Web Application Security: Cloud Portal is static website secured and delivered through CloudFront CDN. LocknCharge's application can be accessed only via HTTPS. We use industry standard encryption for data in transit. All user input is properly encoded when displayed to ensure XSS vulnerabilities are mitigated. Encrypted Data Storage: All data stored in any LocknCharge solutions is encrypted using a 256-bit symmetric algorithm (AES-256-GCM)</p>
<p>NYCRR - 121.9 (a)(8):</p>	<p>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.</p>	<p>Affirm</p>
<p>NYCRR - 121.9 (a)(b):</p>	<p>Describe how the organization will supervise its subcontractors to ensure that as subcontractors perform its contractual obligations, the subcontractor will conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure.</p>	<p>Not applicable - We do not and will not use subcontractors to deliver any of our services.</p>
<p>NYCRR - 121.10 (a):</p>	<p>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.</p>	<p>Our employees are trained in how to communicate incidents internally and our customers are kept informed of incidents that affect their service. In cases that affect a small subset of our customers we may reach out directly to those affected customers.</p>
<p>NYCRR - 121.10 (f):</p>	<p>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.</p>	<p>Affirm</p>
<p>NYCRR - 121.10 (f.2):</p>	<p>Please identify the name of your insurance carrier and the amount of your policy coverage.</p>	
<p>NYCRR - 121.10 (c):</p>	<p>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.</p>	<p>Affirm</p>
<p>Acceptable Use Policy Agreement:</p>	<p>Do you agree with the Capital Region BOCES Acceptable Use Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=B U4QYA6B81BF)</p>	<p>I Agree</p>
<p>Privacy Policy Agreement:</p>	<p>Do you agree with the Capital Region BOCES Privacy Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=B WZSQ273BA12)</p>	<p>I Agree</p>

Parent Bill of Rights:	Please upload a signed copy of the Capital Region BOCES Parent Bill of Rights. A copy of the Bill of Rights can be found here: https://www.capitalregionboces.org/wp-content/uploads/2021/03/CRB_Parents_Bill_Of_Rights_-_Vendors.pdf	CRB Parents Bill Of Rights Vendors - Lockncharge Technologies.pdf
DPA Affirmation:	By submitting responses to this Data Privacy Agreement the Contractor agrees to be bound by the terms of this data privacy agreement.	I Agree

Attachments				
Name	Size	Type	Upload Date	Downloads
CRB Parents Bill Of Rights Vendors - Lockncharge Technologies.pdf	240830	.pdf	12/22/2022 3:03 PM	0
Security and Compliance at LockNCharge.pdf	78245	.pdf	12/22/2022 3:03 PM	1

Comments				
Question Name	Submitter	Date	Comment	Attachment
No Records Found				

Vendor Portal Details			
Contact Name:	The Risk Mitigation & Compliance Office	Publish Date:	
Required Portal Fields Populated:	Yes	Contact Email Address:	crbcontractsoffice@neric.org
About NYCRR Part 121:	In order for a vendor to engage with a New York State Educational Agency, the vendor must provide information required by the New York State Commissioner’s Regulations Part 121 (NYCRR Part 121) and the National Institute of Standards and Technology Cyber Security Framework. If deemed appropriate, the responses you provide will be used as part of the data privacy agreement between the vendor and the Albany-Schoharie-Schenectady-Saratoga BOCES. This Data Privacy Agreement ("DPA") is by and between the Albany-Schoharie-Schenectady-Saratoga BOCES ("EA"), an Educational Agency, and Lock N Charge Technologies LLC ("CONTRACTOR"), collectively, the “Parties”. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.	Requesting Company:	Capital Region BOCES
Created By:		Third Party Name:	Lock N Charge Technologies LLC
		Name:	Lock N Charge Technologies LLC-300812