


Directions

Below is the Third Party contact that will fill out the Part 121 questionnaire. If this is accurate, click the blue "Publish" button. If not, select the appropriate contact by clicking "Lookup" or create a new contact by clicking "Add New".

Vendor Compliance Contacts

Name (Full)	Email	Phone	Third Party Profile
Bjorn Larson	bjorn.larson@maps101.com		Maps.com LLC

General Information

Third Party Profile:	Maps.com LLC	Overall Status:	Approved
Questionnaire ID:	310306	Progress Status:	 100%
Engagements:	Maps101 (DREAM) 23-24	Portal Status:	Vendor Submission Received
Due Date:	5/24/2023	Submit Date:	5/9/2023
		History Log:	View History Log

Review

Reviewer:		Review Status:	Approved
		Review Date:	5/9/2023
Reviewer Comments:			

Data Privacy Agreement and NYCRR Part 121

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?

The exclusive purpose for which the student, teacher, and principle data will be use solely for the purpose of identifying the user, specifically for logging in to the maps101 digital learning platform, and for no other purpose whatsoever.

**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)?

Maps101 has strict policies in place regarding the use of subcontractors in relation to all sensitive data, especially with student, teacher, and principal data. Our subcontractors will not have access to such data and will only be authorized to perform specific tasks on our behalf, such as providing technical support or hosting our digital learning platform. Any subcontractors or other authorized persons or entities to whom the third-party contractor will disclose student data, teacher data, or principal data will be required to agree to strict confidentiality agreements and adhere to 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 take the protection of our users' data very seriously and are committed to ensuring that all of our subcontractors and third-party contractors meet our high standards for data security and privacy.

**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)

Our standard contracts with educational agencies are annual and can be terminated upon request by the agency. If a contract is terminated, any and all personal student, teacher, or principal data that we hold in our system will be permanently deleted, subject to any legal or regulatory requirements that may apply. We understand the importance of data security and privacy, and we take steps to ensure that all data is securely destroyed and any copies that may have been provided to third parties are also securely destroyed.

In terms of the contract's expected commencement and expiration date, this will vary depending on the specifics of the agreement with the educational agency. Our contracts typically begin at the start of the academic year and run for one year, but we are open to negotiating different start and end dates depending on the agency's needs.

In the event that no contract applies, educational agencies may terminate our services at any time upon request. Upon termination, any student data, teacher data, or principal data that we hold in our system will be permanently deleted, subject to any legal or regulatory requirements that may apply.

**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?

We believe that transparency is key to building trust with our users, and we strive to make it easy for all users including parents, students, teachers, and principals to access and manage their data. Users can view their data at any time by accessing their account information, and they can update their name themselves as needed. If a user notices any discrepancies in their data, they can contact our support team to request an update to their email information or to challenge the accuracy of any other data that we have collected.

To challenge the accuracy of student, teacher, or principal data, users can contact our support team directly by phone or email. We will investigate any reported inaccuracies promptly and take steps to correct any errors that are identified. We are committed to maintaining accurate records and to ensuring that all data is handled in accordance with applicable laws and regulations.

**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.

We take data security and privacy very seriously, and we have implemented a number of measures to protect the student data, teacher data, and principal data that we collect. All user data is stored on an encrypted server to prevent unauthorized access, and we use industry-standard encryption algorithms to protect all data in transit.

In addition to encryption, we implement strict access controls to ensure that only authorized personnel are able to access user data. All employees and contractors who handle user data are required to undergo rigorous background checks and training to ensure that they understand and comply with our data security and privacy policies.

We also perform regular security audits and penetration testing to identify and address any potential vulnerabilities in our system. We are committed to staying up-to-date with the latest security best practices and to continuously improving our security posture to mitigate data security and privacy risks.

**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.

We have implemented a number of measures to protect sensitive data both at rest and in motion. All user data is stored on an encrypted server using industry-standard encryption algorithms that are designed to protect data confidentiality and integrity.

When data is in motion, we use secure communication protocols such as HTTPS to ensure that all data is transmitted securely between users and our servers. This helps to prevent unauthorized interception and access to sensitive data while it is in transit.

We also follow best practices for encryption key management, including storing keys in secure hardware devices and limiting access to authorized personnel only. This helps to ensure that encryption keys are not compromised or lost, which could potentially lead to unauthorized access to sensitive data.

Regarding your question about FIPS 140-2 compliance, we utilize encryption algorithms that are compliant with FIPS 140-2. We recognize the importance of this standard in protecting sensitive data and take steps to ensure that all of our encryption algorithms comply with these standards.

**NYCRR - 121.6
(a):**

Please submit the organization's data security and privacy plan that is accepted by the educational agency.

Privacy Policy - Maps101, Inc 2023.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.

We are committed to staying up to date and implementing all applicable 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.

We have policies and procedures that are designed to protect the confidentiality, integrity, and availability of all data that we collect and process. These policies and procedures are reviewed and updated on a regular basis to ensure that they remain current and effective in addressing emerging security and privacy risks.

We also follow industry best practices for data security and privacy, including data encryption, access controls, monitoring and logging, and incident response planning. Our security and privacy controls are regularly audited and tested by third-party assessors to ensure that they are operating effectively and in compliance with relevant laws and regulations.

In addition, we have established a clear process for reporting and responding to security and privacy incidents, including breach notification and mitigation procedures. We work closely with educational agencies to ensure that all incidents are promptly reported and appropriately addressed.

We understand the importance of protecting sensitive data and take our responsibility to safeguard such data very seriously. We are committed to working closely with educational agencies to ensure that all data security and privacy contract requirements are met over the life of the contract.

**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.

We take the protection of personally identifiable information (PII) very seriously. To ensure the security and privacy of PII that we receive under the engagement, we have implemented a range of administrative, operational, and technical safeguards and practices, including:

- **Administrative Safeguards:** We have implemented policies and procedures that are designed to ensure that all PII is handled and processed in accordance with relevant laws and regulations, including FERPA and other applicable data privacy and security regulations. We also provide regular training to our staff to ensure that they understand and comply with these policies and procedures.
- **Operational Safeguards:** We have established clear guidelines and procedures for how PII is collected, stored, and processed. We also limit access to PII to only those employees who need access to perform their job duties. We use secure protocols to transmit PII over the Internet and require all vendors and third-party service providers to adhere to the same security and privacy standards that we have in place.
- **Technical Safeguards:** We use a range of technical safeguards to protect PII from unauthorized access, use, or disclosure. These include encryption of all PII at rest and in transit, strong access controls, monitoring and logging of all system activity, and regular vulnerability scanning and testing.

We also use third-party assessments to ensure the effectiveness of our security and privacy controls. These assessments typically include vulnerability assessments and penetration testing to identify and address any security weaknesses. We also conduct periodic audits to ensure compliance with all relevant laws and regulations.

**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.

We have implemented various measures to ensure that our employees and assignees are well-informed on the Federal and State laws governing the confidentiality of such data. Prior to being granted access to such data, officers and employees are required to undergo extensive training on the applicable privacy and data protection laws and regulations. This training covers topics such as the types of data that are considered confidential, the legal requirements for handling such data, and the consequences of mishandling or disclosing such data improperly.

In addition to initial training, we provide ongoing training and updates to all personnel who have access to such data to ensure that they remain up-to-date on the latest privacy and security requirements. Our training programs are designed to ensure that all personnel who have access to sensitive data understand the importance of maintaining the confidentiality and security of such data.

We also have implemented various administrative, operational, and technical safeguards and practices to protect personally identifiable information. These include restricting access to sensitive data to only authorized personnel, implementing secure access controls and password policies, and conducting periodic audits to ensure compliance with all relevant laws and regulations. Additionally, we may use third-party assessments to verify the effectiveness of our privacy and data protection measures, and such assessments may include penetration testing and vulnerability assessments.

**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.

We do use sub-contractors in some cases, but the security and privacy of personally identifiable information is always a top priority. We have stringent contract requirements for all sub-contractors that mandate their compliance with all applicable data privacy and security laws and regulations, including FERPA.

To ensure that our sub-contractors adhere to our standards, we conduct a thorough evaluation of their privacy and security policies, procedures, and practices. We also maintain ongoing monitoring and oversight of our sub-contractors to ensure that they remain compliant with all relevant laws and regulations.

Our contracts with sub-contractors include provisions for data security, confidentiality, and data protection, which require them to implement administrative, physical, and technical safeguards to protect the personally identifiable information of our clients. Additionally, we maintain a separate staging environment for most sub-contractor work where sensitive data is not accessible to them.

Periodic audits are conducted to ensure that our sub-contractors fulfill their contractual obligations and maintain the security and privacy of personally identifiable information.

**NYCRR - 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.

We have implemented policies and procedures to manage such incidents in a timely and effective manner. Our incident management plan includes specific steps to identify breaches and unauthorized disclosures, contain the incident, mitigate potential damage, and notify the educational agency promptly.

We have a team of trained incident response professionals who are responsible for managing incidents that implicate personally identifiable information. This team includes members from various departments, including IT, legal, and senior management. They work together to investigate incidents and take appropriate action to remediate the situation.

If a breach or unauthorized disclosure occurs, we will promptly notify the educational agency and any affected individuals in accordance with applicable laws and regulations. Our notification procedures include providing detailed information about the incident, the type of data that was compromised, and steps that affected individuals can take to protect themselves.

<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>At the end of our engagement, we will work with the educational agency to ensure that all data is handled in accordance with the terms of the contract and applicable laws and regulations.</p> <p>If the user data is no longer needed and is requested to be deleted by the educational agency, we will comply with those instructions and provide documentation such as a Data Destruction Affidavit to confirm the proper destruction of data. We understand the sensitivity of data and the importance of ensuring that it is protected throughout the entire lifecycle, including at the end of our engagement.</p>
<p>NYCRR - 121.9 (a)(1):</p>	<p>Is your organization compliant with the NIST Cyber Security Framework?</p>	<p>Yes</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>Maps101 is committed to complying with the data security and privacy policy of the educational agency we contract with, as well as Education Law section 2-d and all relevant regulations. To achieve this, we have established a comprehensive data security and privacy program that incorporates administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of student and educator data.</p> <p>Our program includes policies and procedures for data access, handling, retention, and disposal, as well as guidelines for incident response and breach notification. We regularly assess and update our program to ensure that it remains current and effective in light of emerging threats and changes in the regulatory landscape.</p> <p>We also work closely with our educational agency partners to understand their specific data security and privacy requirements and tailor our program to meet their needs. We conduct regular training and awareness programs for our employees and contractors to ensure they understand the importance of safeguarding student and educator data, as well as the legal and regulatory obligations that apply.</p> <p>Finally, we engage in ongoing monitoring and auditing of our program to ensure compliance with all applicable laws, regulations, and contractual obligations. We are committed to maintaining a culture of data security and privacy throughout maps101 and among our partners to protect the sensitive information we handle.</p>

**NYCRR - 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 authorized access to provide services.

We understand the importance of limiting internal access to personally identifiable information (PII) only to those employees or sub-contractors who need authorized access to provide services. We have implemented strict policies and procedures to ensure that PII is only accessible to those individuals who require it to perform their job duties.

To accomplish this, we have implemented role-based access controls that restrict access to PII based on an individual's job responsibilities and the minimum necessary information needed to perform their job. Our employees and sub-contractors are only granted access to PII on a need-to-know basis and are required to complete specialized training on data protection and privacy before being granted access.

We also conduct regular audits and reviews of our access controls to ensure that only authorized individuals have access to PII. Additionally, all employees and sub-contractors must sign confidentiality agreements that prohibit the unauthorized use or disclosure of PII, and any suspected incidents of unauthorized access are promptly investigated.

Overall, we take the protection of PII very seriously and have implemented a comprehensive system of policies, procedures, and controls to ensure that internal access is limited to only those individuals who require it to provide services.

**NYCRR - 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. (e.g. Role Based Access, Continuous System Log Monitoring/Auditing)

To control access to protected data and ensure that personally identifiable information is not used for any purpose not explicitly authorized in our contract, there are several measures that can be taken.

One effective approach is to implement a Role-Based Access Control (RBAC) system. This allows Maps101 to define and manage different roles, and grant access to data based on an individual's job responsibilities and level of clearance. RBAC ensures that only authorized individuals can access sensitive information and limits the potential for unauthorized use or disclosure.

In addition to RBAC, continuous system log monitoring and auditing can be employed to track access to the protected data. This involves monitoring and analyzing logs generated by our systems to identify any suspicious activity or unauthorized access attempts. This provides an additional layer of security and helps detect and prevent any potential data breaches.

**NYCRR - 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.

To ensure that personally identifiable information is not disclosed to any other party without the prior written consent of the parent or eligible student, we implemented the following measures:

Firstly, we will ensure that any third-party contractors, such as subcontractors or assignees, who may require access to the personally identifiable information to carry out the contract, are authorized representatives and comply with state and federal laws, regulations and our contracts with the educational agency. This will include having appropriate confidentiality and data protection provisions in their contract and ensuring that the third-party contractors have adequate security measures in place to protect the data.

Secondly, if there is a statutory or court order that requires disclosure of the personally identifiable information, we will provide 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. This will allow the educational agency to take necessary measures to protect the confidentiality of the information and ensure compliance with any legal requirements.

Overall, by implementing these measures, we ensure that personally identifiable information is only disclosed in situations where it is required by law or where the parent or eligible student has provided prior written consent. This will help safeguard the privacy and confidentiality of student information, and demonstrate our commitment to compliance with legal and regulatory requirements.

**NYCRR - 121.9
(a)(6):**

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.

To maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody, we implemented the following measures:

Administrative safeguards: We established policies, procedures, and guidelines for the collection, storage, use, and disclosure of personally identifiable information. These policies and procedures will be communicated to employees, contractors, and other stakeholders, and regular training will be provided to ensure that they understand their roles and responsibilities in protecting the data.

Technical safeguards: we implemented appropriate security measures, such as access controls, encryption, firewalls, and intrusion detection and prevention systems, to prevent unauthorized access to the personally identifiable information. Regular security assessments will be conducted to identify and address any vulnerabilities or weaknesses in our systems' and processes.

Physical safeguards: We implemented physical security measures, such as locks, alarms, surveillance cameras, and restricted access controls, to protect the physical storage and handling of personally identifiable information. We also implemented secure disposal procedures for any physical documents or storage media that contain personally identifiable information.

Monitoring and incident response: We implemented continuous monitoring and auditing of its systems and processes to detect and respond to any security incidents or breaches. We also have an incident response plan in place, which outlines the steps to be taken in the event of a security incident or breach.

Overall, by implementing these measures, we will maintain the confidentiality, integrity, and security of personally identifiable information in its custody. This will help prevent unauthorized access, use, or disclosure of the data and ensure compliance with legal and regulatory requirements related to data privacy and security.

**NYCRR - 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.

To protect personally identifiable information (PII) in its custody while in motion or at rest, we implemented encryption as a key security measure. The following measures will be taken to ensure that encryption is used effectively:

Use of strong encryption algorithms: We ensure that encryption algorithms used to protect PII are strong and not vulnerable to attack. We regularly review and update encryption protocols to ensure that they meet industry standards.

Encryption of data in motion: All PII transmitted across networks or other communication channels will be encrypted using secure encryption protocols, such as SSL or TLS. This will ensure that any sensitive data sent over the internet or other networks is protected against unauthorized interception and access.

Encryption of data at rest: All PII stored in databases or other storage media will be encrypted using strong encryption algorithms. This will ensure that any sensitive data that is stored on devices, servers, or databases is protected against unauthorized access, even if the physical device is lost or stolen.

Secure key management: We implemented secure key management practices to ensure that encryption keys used to protect PII are managed securely and cannot be accessed by unauthorized parties.

**NYCRR - 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.

Affirm

**NYCRR - 121.9
(a)(b):**

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.

To ensure that subcontractors conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure, the maps101 has established the following procedures, which includes policies and procedures for selecting, monitoring, and supervising subcontractors who have access to protected data.

We conduct a thorough vetting process to select subcontractors that have a proven track record of complying with State and Federal laws related to data security. We require potential subcontractors to provide evidence of their compliance, including any relevant certifications, licenses, or audits.

Once selected, subcontractors will be required to sign a comprehensive data security agreement that outlines their specific obligations to protect our data. This agreement will include requirements for implementing appropriate technical, physical, and administrative safeguards to protect against unauthorized access, use, and disclosure of protected data.

To monitor subcontractor compliance with these requirements, we conduct periodic audits and assessments of their security controls and practices. We will also require subcontractors to promptly report any security incidents or breaches to Maps101, and will provide them with guidance and support to address any issues that arise.

We are committed to ensuring that subcontractors perform their contractual obligations in a manner that conforms with State and Federal laws related to data security. Through a comprehensive subcontractor management program, we will mitigate the risk of data breaches and ensure the confidentiality, integrity, and availability of its protected data.

<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>We understand the importance of promptly notifying each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information. To ensure that this notification process is carried out in a timely and efficient manner, we have established a comprehensive breach notification policy.</p>
		<p>As soon as we become aware of any breach or unauthorized release of personally identifiable information, it will immediately initiate an investigation to determine the scope and cause of the incident. Once we confirm that a breach has occurred, it will notify the affected educational agency within seven calendar days, or as soon as possible without unreasonable delay.</p>
		<p>We will communicate the details of the breach to the educational agency, including the types of data affected, the number of individuals affected, the potential risks or harms resulting from the breach, and any remedial actions that we have taken or plans to take to address the breach.</p>
		<p>We will also work closely with the affected educational agency to provide any additional support or assistance that may be needed, such as providing credit monitoring services or offering guidance on how to mitigate the risks associated with the breach.</p>
		<p>Overall, Maps101 is committed to maintaining the privacy and security of personally identifiable information and will take all necessary measures to ensure that breaches are promptly identified, investigated, and reported to the affected educational agencies in accordance with State and Federal laws and regulations.</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>Scott Insurance Company \$1M Policy</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	Capital Region BOCES Parent Bill of Rights - Maps101 Signed 2023.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
No Records Found				

Comments				
Question Name	Submitter	Date	Comment	Attachment
No Records Found				

Vendor Portal Details	
Contact Name:	The Risk Mitigation & Compliance Office
Required Portal Fields Populated:	Yes
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 Maps.com 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.
Created By:	Yaeger, KellyRose
Publish Date:	
Contact Email Address:	crbcontractsoffice@neric.org
Requesting Company:	Capital Region BOCES
Third Party Name:	Maps.com LLC
Name:	Maps.com LLC-310306