

GARDEN CITY UNION FREE SCHOOL DISTRICT

EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Incident IQ (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the GARDEN CITY UNION FREE SCHOOL DISTRICT (the "District") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"Protected Data" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

"Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,

-AND-

"Personally identifiable information" from the records of the District 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of

Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;
2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;
3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
5. Specifies how Contractor 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;
6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract;
5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student:
 - a. except for authorized representatives 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. unless required by statute or court order and Contractor has provided 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.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody;
7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and
8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

NAME OF PROVIDER: Incident IQ, LLC

BY: Donato Latrofa **DATED:** 5-20-24

Donato Latrofa
General Counsel

Return to:

Lauren Maguire
Director of Information Technology
Garden City Union Free School District
56 Cathedral Avenue
Garden City, NY 11530
maguirel@gcufsd.net

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

Incident IQ
DATA PRIVACY AND SECURITY PLAN

Incident IQ, LLC (“Incident IQ, We, Us, or Our”), as a covered third-party contractor under NYS Education Law 2-d shall undertake all of the following data privacy, security, and protection measures, in addition to the requirements already contained in the Incident IQ Cloud Services Master Subscription Agreement (available at <https://www.incidentiq.com/legal>):

1. Data Collection & Use:

- a. Incident IQ shall only collect only collect, process and store such Protected Data, to include any cookies, to which we have a legitimate educational interest and as is necessary to provide the cloud services.
- b. Under no circumstances will Incident IQ use Protected Data to market or advertise to students or their family members or legal guardians, or otherwise use Protected Data to inform, influence or enable marketing, advertising or other commercial efforts by a third party directed at students, their family members, or legal guardians.
- c. We shall not change how Protected Data are collected maintained, used or disclosed under the terms of the Agreement, without advance notice to and prior written consent from District.
- d. We will never sell Protected Data that we acquire through District use of the Cloud Services, except as part of a corporate purchase, merger or other type of acquisition. In such a case, any successor entity shall be contractually obligated to comply with the terms of this Agreement related to the treatment of Protected Data, as well as all other applicable legal requirements governing the use, disclosure, and security of the previously acquired Protected Data.

2. Data Portability: Incident IQ shall ensure the data portability of all District data.

- a. Upon notice of a request from District for a copy of certain Protected Data in Our possession (e.g., to support the District’s response to a properly constituted request for Protected Data from a parent, guardian or student), we will ensure that: (i) A complete and readable digital copy of the requested Protected Data in Incident IQ’s possession is delivered to District within 30 days of our receipt of District’s request; (ii) Upon delivery of the copy, District must provide notice to Incident IQ of District’s receipt and acceptance of any such requested Protected Data;
- b. Upon notice of a request from District that certain Protected Data be deleted, We will permanently destroy (i.e., undertake a non-recoverable deletion process in accordance with Department of Defense standard 5220.22-M) all copies of the Protected Data identified for deletion by District held by Us or any of Our agents, subcontractors or affiliates. Within 30 days of District notice, we will deliver a written confirmation to District certifying that the permanent destruction of the requested Protected Data has been accomplished. Upon delivery of such written confirmation of deletion, District must provide notice to Us of District receipt and understanding of said notice confirming deletion made at District request.
- c. We shall destroy all Protected Data residing in District’s instance of the Cloud Services, using the methods described in paragraph 2(b) above, following expiration of a 60-day period after termination of this Agreement, unless District requests that We return such information to District instead.

3. Data Security:

- a. We will operate the Cloud Services and collect, process and store Protected Data in accordance with NIST data security standards and current industry best practices, and maintain all technologies, policies, procedures and practices necessary to secure and protect the confidentiality and integrity of Protected Data, and prevent unauthorized access, disclosure and use.
- b. All information is stored within databases hosted and secured within the Microsoft Azure Cloud. The Azure cloud is secured with actively monitored network firewalls, intrusion detection systems, application firewalls, and IP-route protection. Additionally, any information designated as Protected Data is encrypted within the database.
- c. No data shall be stored outside the United States; all data are stored in the Microsoft Azure data center, region East US (Virginia), East US 2 (Virginia), and/or West US (California).
- d. Any data designated as Protected Data which include passwords, is encrypted within the database using combinations of one-way and two-way encryption algorithms (such as SHA256) with Salt strings.
- e. Information is multi-tenanted and stored within the same cloud systems; however, all information is partitioned by a School District ID (i.e., SiteId) and the Data Access Layers forces all data to be filtered by a specific School District.
- f. Physical servers are physically secured in the Microsoft Azure data centers, regions East US (Virginia), East US 2 (Virginia), and West US (California).
- g. Data in transit are SSL protected, as well as Protected Data are always encrypted.
- h. Only Incident IQ Senior Technical Team members have direct access to product data. All personnel with access to Incident IQ systems and data are vetted via backgrounds checks and receive annual and update training on all relevant policies and procedures.
- i. No software functions are subcontracted to other vendors apart from the hosting/storage services provided by Microsoft, as described above.
- j. Customer support representatives accordingly confirm caller identity against a District's list of administrator-users. Account creation and deletion is controlled by the District as user profiles are established through syncing with the client's identity management provider (e.g., Microsoft ADFS, Google SSO, local Active Directory, etc.). Accordingly, account creation/deletion is managed by the District through their ordinary identity management policies and procedures. Also, permissions modification of any given user may be managed by the clients' administrator-level users through tools in their admin console. If assistance were required in this process admin-users would authenticate with customer support representatives as described above.

4. Network Operations Center Management and Security:

- a. Incident IQ shall perform regular penetration testing, vulnerability management and intrusion prevention testing.
- b. All network devices shall be located in secure facilities under controlled circumstances (*i.e.*, ID cards and entry logs) at the Microsoft Azure data centers, regions East US (Virginia), East US 2 (Virginia), and West (California).
- c. Backups shall be performed daily (to other US-based Azure Data Centers), as well as backups made to separate secure, off-site facility.
- d. Backups shall be encrypted and stored securely with access limited to administrators with restoration encryption keys.
- e. All software vulnerabilities shall be patched routinely or automatically in accordance with the following parameters: all critical and High vulnerabilities shall be patched automatically. Medium vulnerabilities shall be patched monthly during planned maintenance windows. Low vulnerabilities shall be evaluated and if deemed necessary, shall be patched during the planned monthly maintenance window.
- f. Incident IQ shall respond to any incidents IAW its Incident Response Plan.

**GARDEN CITY UNION FREE SCHOOL DISTRICT
PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

Pursuant to New York State Education Law § 2-d, parents, legal guardians and persons in parental relation to a student are entitled to certain rights with regard to their child's personally identifiable information, as defined by Education Law § 2-d. This document contains a plain English summary of such rights.

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 educational records maintained by the Garden City Public Schools.
3. State and Federal Laws protect the confidentiality of personally identifiable student 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 review at the following website:

<http://www.p12.nysed.gov/irs/sirs>

The list may also be made available by writing to:

Office of Information & Reporting Services
New York State Education Department
Room 863 EBA,
89 Washington Avenue
Albany, NY 12234

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:

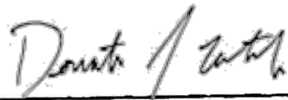
Garden City Public Schools
Att. Mrs. Lauren Maguire,
Data Protection Officer
56 Cathedral Ave.
Garden City, NY 11530

OR

Chief Privacy Officer
New York State Education Department
89 Washington Avenue Albany,
NY 12234
Email: Privacy@nysed.gov

6. Each contract with a third-party contractor which will receive student data, or teacher or principal data will include supplemental information addressing the following:
 - a. The exclusive purposes for which the student data or teacher or principal data will be used.
 - b. How the third-party contractor will ensure that the subcontractors, persons or entities that the third-party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.
 - c. When the agreement expires and what happens to the student data or teacher and principal data upon expiration of the agreement.
 - d. If and how a parent, student, a student over eighteen years of age, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
 - e. 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; and
 - f. Address how the data will be protected using encryption while in motion and at rest.
 7. Under Section 2-d, 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. Except for authorized representative of the third party contractor to the extent they are carrying out the contract, not disclose personally identifiable information to any other party (i) 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 Garden City Public Schools 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 Garden City Public Schools 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.



Signature

Donato Latrofa

Print Name

Incident IQ, LLC

Provider

5-20-24

Date

General Counsel

Title

750 Glenwood Ave SE, Suite 320
Atlanta, GA 30316

Address



Quote Name Garden City Public Schools - NY - [A,T,PM] - Platform Renewal Created Date 3/8/2024
Company Address 750 Glenwood Ave SE Suite 320 Expiration Date 6/29/2025
Atlanta, GA 30316 Quote Number 40450
US
Contract Start Date 7/1/2024
Contract End Date 6/30/2025

Bill To 56 Cathedral Avenue
Garden City, NY

Product Code	Product	Product Description	Sales Price	Quantity
IIQ-6200	iiQ Assets	Incident IQ Assets product (add-on), Subscription	REDACTED	
IIQ-8700	iiQ LocknCharge Integration	Incident IQ Integration with LocknCharge FUYL Tower (add-on)	REDACTED	
IIQ-1000	iiQ Platform with Ticketing	Incident IQ Platform with iiQ Ticketing core product, Subscription	REDACTED	
IIQ-8100	iiQ Policy Manager	Incident IQ Policy Manager (add-on), Subscription	REDACTED	
Total Price			REDACTED	

Notes

Current subscription ends June 30, 2024. Above quoted license begins July 1, 2024 and ends on June 30, 2025.