OAKLAND UNIFIED SCHOOL DISTRICT
Community Schools, Thriving Students

Board Office Use: **Legislative File Info.**	
File ID Number	24-1081
Introduction Date	5/22/24
Enactment Number	
Enactment Date	

Board Cover Memorandum

To	Board of Education
From	Kyla Johnson-Trammell, Superintendent Preston Thomas, Chief Systems and Services Officer Susan Beltz, Chief Technology Officer
Meeting Date	May 22, 2024
Subject	Ratification of Student Data Privacy Agreement between Incident IQ, Inc. and Oakland Unified School District Contractor: Incident IQ Services For: April 17, 2024 - June 30, 2025

Ask of the Board	☐Approve Data Privacy Agreement ☑Ratify Data Privacy Agreement
Services	Incident IQ, Inc. will provide a support ticketing, asset management, and human resources workflow management platform to better enable the Technology Services, Talent, and other departments to more efficiently respond to requests from OUSD staff and students and manage internal processes. The platform may hold student information as necessary in order to fulfill a particular support request, necessitating a data privacy agreement.
Term	Start Date: April 17, 2024 End Date: June 30, 2025
Not-To-Exceed Amount	N/A
Competitively Bid	No. Data Privacy Agreement
In-Kind Contributions	No in-kind contributions
Funding Source(s)	N/A

Background

Incident IQ, Inc. will provide a support ticketing, asset management, and human resources workflow management platform to better enable the Technology Services, Talent, and other departments to more efficiently respond to requests from OUSD staff and students and manage internal processes.

In order to provide these services, Learning Genie may require access to certain District student data as needed in order to fulfill a particular support request. Accordingly, the District and Incident IQ executed the enclosed data sharing agreement on 04/17/2024, and now ask the Board to ratify this agreement.

This data sharing agreement is the standard California - National Student Data Privacy Agreement (CA-NDPA), adopted by the California Student Privacy Alliance to meet the requirements of the Family Educational Rights and Privacy Act (FERPA) and Assembly Bill 1584 (which allows school districts to share data with software providers so long as the contracts include certain specified provisions).

The standard terms of the CA-NDPA ensure that the vendor will take all precautions to safeguard our students' data. The term of the CA-NDPA is the same as the term of the underlying services agreement.

The CA-NDPA is a piggy-backable agreement. This means that a software vendor may enter the CA-NDPA with one school district and thereafter, by signing Exhibit E (which consists of a "general offer of terms") allow any other school district to countersign Exhibit E and be entitled to the same protections set forth in the underlying CA-NDPA.

Here, Incident IQ has signed the CA-NDPA with the Oak Park Unified School District, and it further signed Exhibit E, which, again, allows any other school district to likewise sign Exhibit E and share the same data with Incident IQ under the same terms. Accordingly, the District signed Exhibit E on 04/17/2024, and now asks the Board to ratify this agreement.

Attachment(s)

- Incident IQ, Inc. California National Student Data Privacy Agreement with Exhibit E
- Incident IQ, Inc. Terms of Service Agreement

STANDARD STUDENT DATA PRIVACY AGREEMENT

CA-NDPA Standard
Version 1.0

Oak Park Unified School District

and

Incident IQ, LLC

02/05/2021

This Student Data Privacy Agreement ("**DPA**") is entered into on the date of full execution (the "**Effective Date**") and is entered into by and between:

Oak Park Unified School District , located at

(the "**Local Education Agency**" or "**LEA**") and

Incident IQ, LLC , located at 519 Memorial Drive SE, Ste B-12, Atlanta, GA 30312

(the "**Provider**").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 CFR Part 99);
the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations

and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. **Special Provisions.** ***Check if Required***

   ☑ If checked, the Supplemental State Terms and attached hereto as **Exhibit "G"** are hereby incorporated by reference into this DPA in their entirety.

   ☑ If Checked, the Provider, has signed **Exhibit "E"** to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three years. Exhibit E will expire 3 years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in **Exhibit "A"** (the "**Services**").

6. **Notices.** All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the Provider for this DPA is:

Name: R.T. Collins Title: COO

Address: 519 Memorial Drive SE, Ste B-12, Atlanta, GA 30312

Phone: (470) 737-3505 Email: rtcollins@incidentiq.com

The designated representative for the LEA for this DPA is:

Name: Enoch Kwok Title: Director of Technology

Address: 5801 Conifer St., Oak Park, CA 91377

Phone: (818) 735-3200 Email: technology@opusd.org

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA: Oak Park Unified School District

By: _____ Date: 2/18/2021

Printed Name: Adam Rauch Title/Position: Asst. Superintendent Business Services

PROVIDER: Incident IQ, LLC

By: _____ Date: 02/05/2021

Printed Name: R.T. Collins Title/Position: COO

STANDARD CLAUSES
Version 1.0

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit "B".**

3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit "C".** In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. **Subprocessors.** Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Rrecords and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. **Unauthorized Access Notification.** LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit A or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non-public information and/or personally identifiable information contained in the Student Data other than as directed or

permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. **De-Identified Data:** Provider agrees not to attempt to re-identify de-identified Student Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which de-identified data is presented.

6. **Disposition of Data.** Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a "Directive for Disposition of Data" form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ Exhibit "D," no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit "D.

7. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.

2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA . The Provider will cooperate reasonably with the LEA and any local, state, or federal

agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth set forth in **Exhibit "F".** Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H".** Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F".** Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.

4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:

   (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:

      i. The name and contact information of the reporting LEA subject to this section.
      ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
      iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
      iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
      v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

   (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

   (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of "General Offer of Privacy Terms" (General Offer, attached hereto as **Exhibit "E"**), be bound by the terms of **Exhibit "E"** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.

3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between Exhibit H, the SDPC Standard Clauses, and/or the Supplemental State Terms, Exhibit H will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. **Waiver.** No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF PRODUCTS AND SERVICES HERE.
IF MORE THAN ONE PRODUCT (RESOURCE) OR SERVICE IS INCLUDED, LIST EACH PRODUCT (RESOURCE) HERE]

Incident IQ cloud software as a service platform with service modules for IT Incident ticketing (SKU IIQ-1000) and IT asset management (SKU IIQ-6200), as well as related professional services for software implementation and training (SKU IIQ-9000).

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	✔
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	✔
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	✔
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	✔
	Student grade level	✔
	Homeroom	✔
	Guidance counselor	✔
	Specific curriculum programs	
	Year of graduation	✔
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	✔
	Email	✔
	Phone	✔

Category of Data	Elements	Check if Used by Your System
Parent/Guardian ID	Parent ID number (created to link parents to students)	✔
Parent/Guardian Name	First and/or Last	✔
Schedule	Student scheduled courses	✔
	Teacher names	✔
Special Indicator	English language learner information	
	Low income status	
	Medical alerts/ health data	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	✔
	Email	✔
	Phone	✔
Student Identifiers	Local (School district) ID number	✔
	State ID number	✔
	Provider/App assigned student ID number	✔
	Student app username	✔
	Student app passwords	
Student Name	First and/or Last	✔
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	✔
Student work	Student generated content; writing, pictures, etc.	✔
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	

Category of Data	Elements	Check if Used by Your System
	Other transcript data - Please specify:	☐
Transportation	Student bus assignment	☐
	Student pick up and/or drop off location	☐
	Student bus card ID number	☐
	Other transportation data – Please specify:	☐
Other	Please list each additional data element used, stored, or collected by your application:	☐
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

EXHIBIT "C"
DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be de-identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student's identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student's cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an "operator" for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term "Provider" includes the term "Third Party" and the term "Operator" as used in applicable state statutes.

Student Generated Content: The term "student-generated content" means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of personally identifiable information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to,

information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "personally identifiable information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data.

Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

Oak Park Unified School District Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

☐ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

☐ **[Insert categories of data here]**

☐ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

☐ Disposition shall be by destruction or deletion of data.

☐ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

☐ As soon as commercially practicable.

☐ By

4. Signature

_____ _____

Authorized Representative of LEA Date

5. Verification of Disposition of Data

_____ _____

Authorized Representative of Company Date

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

1. Offer of Terms

Provider offers the same privacy protections found in this DPA between it and Oak Park Unified School District ("Originating LEA") which is dated 02/05/2021, to any other LEA ("Subscribing LEA") who accepts this General Offer of Privacy Terms ("General Offer") through its signature below. This General Offer shall extend only to privacy protections, and Provider's signature shall not necessarily bind Provider to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Provider and the Subscribing LEA may also agree to change the data provided by Subscribing LEA to the Provider to suit the unique needs of the Subscribing LEA. The Provider may withdraw the General Offer in the event of: (1) a material change in the applicable privacy statues; (2) a material change in the services and products listed in the originating Service Agreement; or three (3) years after the date of Provider's signature to this Form. Subscribing LEAs should send the signed **Exhibit "E"** to Provider at the following email address:

rtcollins@incidentiq.com

PROVIDER: Incident IQ, LLC

BY: R.T. Collins Date: 02/05/2021

Printed Name: R.T. Collins Title/Position: COO

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the

and the Provider. **PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. **

LEA:

BY: Susan E Beltz Date: 4/17/2024

Printed Name: Susan Beltz Title/Position: Chief Technology Officer

SCHOOL DISTRICT NAME: Oakland Unified School District

DESIGNATED REPRESENTATIVE OF LEA:

Name: Susan Beltz

Title: Chief Technology Officer

Address: 1011 Union Street, Oakland CA 94607

Telephone Number: 510-879-8873

Email: susan.beltz@ousd.org

Pursuant to BP 3312, Provider's standard Terms and Conditions, attached to this item and available at https://www.incidentiq.com/legal/terms-of-use, constitute this separate Service Agreement between Subscribing LEA and Provider.

Approved as to form:

By: Jenine Lindsey 4/17/2024

Jenine Lindsey, Interim General Counsel

EXHIBIT "F"
DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks
2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
☐	National Institute of Standards and Technology	NIST Cybersecurity Framework Version 1.1
☐	National Institute of Standards and Technology	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
☐	International Standards Organization	Information technology — Security techniques — Information security management systems (ISO 27000 series)
☐	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
☐	Center for Internet Security	CIS Critical Security Controls (CSC, CIS Top 20)
☐	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

Please visit http://www.edspex.org for further details about the noted frameworks.

*Cybersecurity Principles used to choose the Cybersecurity Frameworks are located here

EXHIBIT "G"

Supplemental SDPC State Terms for California

Version 1.0

This Amendment for SDPC State Terms for California ("**Amendment**") is entered into on the date of full execution (the "**Effective Date**") and is incorporated into and made a part of the Student Data Privacy Agreement ("**DPA**") by and between:

Oak Park Unified School District, located at (the "**Local Education Agency**" or "**LEA**") and Incident IQ, LLC, located at 519 Memorial Drive SE, Ste B-12, Atlanta, GA 30312 (the "**Provider**").

All capitalized terms not otherwise defined herein shall have the meaning set forth in the DPA.

WHEREAS, the Provider is providing educational or digital services to LEA, which services include: (a) cloud-based services for the digital storage, management, and retrieval of pupil records; and/or (b) digital educational software that authorizes Provider to access, store, and use pupil records; and

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("**FERPA**") at 20 U.S.C. § 1232g (34 C.F.R. Part 99); the Protection of Pupil Rights Amendment ("**PPRA**") at 20 U.S.C. §1232h; and the Children's Online Privacy Protection Act ("**COPPA**") at 15 U.S.C. § 6501-6506 (16 C.F.R. Part 312), accordingly, the Provider and LEA have executed the DPA, which establishes their respective obligations and duties in order to comply with such applicable laws; and

WHEREAS, the Provider will provide the services to LEA within the State of California and the Parties recognizes the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable California laws and regulations, such as the Student Online Personal Information Protection Act ("**SOPIPA**") at California Bus. & Prof. Code § 22584; California Assembly Bill 1584 ("**AB 1584**") at California Education Code section 49073.1; and other applicable state privacy laws and regulations; and

WHEREAS, the Provider and LEA desire to enter into this Amendment for the purpose of clarifying their respective obligations and duties in order to comply with applicable California state laws and regulations.

NOW, THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. **Term**. The term of this Amendment shall expire on the same date as the DPA, unless otherwise terminated by the Parties.

2. **Modification to Article IV, Section 7 of the DPA**. Article IV, Section 5 of the DPA (Advertising Limitations) is amended by deleting the stricken text as follows:

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data ~~(i)~~ for adaptive learning or customized student learning (including generating personalized learning recommendations)~~; or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services~~ or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

[SIGNATURES BELOW]

IN WITNESS WHEREOF, LEA and Provider execute this Amendment as of the Effective Date.

LEA: Oak Park Unified School District

By: _____ Date: 2/18/2021

Printed Name: Adam Rauch Title/Position: Asst. Superintendent Business Services

Provider: Incident IQ, LLC

By: _____ Date: 02/05/2021

Printed Name: R.T. Collins Title/Position: COO

INCIDENT IQ CLOUD SERVICES
ORDER FORM

THIS ORDER FORM FOR CLOUD SERVICES (“ORDER FORM”), ALONG WITH THE APPLICABLE TERMS OF THE MASTER SUBSCRIPTION AGREEMENT AND ANY APPLICABLE EXHIBITS, GOVERN YOUR RENEWAL AND USE OF INCIDENT IQ CLOUD SERVICES (“CLOUD SERVICES”) UNDER THESE TERMS.

BY EXECUTING THIS AGREEMENT YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A SEPARATE LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERMS "YOU" OR "YOUR" SHALL REFER TO SUCH ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE CLOUD SERVICES.

This Agreement was last updated as of January 12, 2023. It is effective between You and Us as of the date You execute this agreement (the “Effective Date”).

1. ORDER FORM AND TABLE OF AGREEMENT

This Order Form as issued by Incident IQ, LLC is an offer by Incident IQ, LLC. When signed and returned to Us by You, it becomes a binding agreement for the Incident IQ Cloud Services listed in this order form and is effective on the date signed by You.

This Order Form is governed by and incorporates the following documents in effect as of the effective date. All documents are listed in order of precedence, and collectively referred to as the “Agreement”:

Document	Location
Order Form (pgs 1-3)	
Incident IQ Cloud Services Master Subscription Agreement, eff. January 8, 2023 (pgs 4-21)	Exhibit 1
Support Policy for Cloud Services (pg 22)	Exhibit 2

2. SERVICES ORDER

The below summarizes the agreed upon initial Services and agreed upon prices and fees purchased by You under the contract as described in the quote to be provided by the third-party CDW, Douglas Stewart**. You are purchasing the following products:**

Platform w/ Ticketing, Assets, EAW, Launchpad

3. TERM AND TERMINATION

3.1. The Services Period for the Cloud Services under this Order Form begins on **March 29, 2024** and expires on **July 8, 2024,** unless otherwise supplemented or amended in writing.

3.2 No rights, access, or authorization to use the Cloud Services or Content enabled by this Order Form, nor any portion thereof, shall Auto-Renew past the date unless expressly agreed to by both parties in writing.

4. PAYMENT AND INVOICES

4.1. Fees and Invoicing. You will provide a Purchase Order to Johnhar@cdwg.com by Apr 3, 2024.

A. All fees will be invoiced by Us and paid by You in advance. Incident IQ may provide invoices to **kyleigh.nevis@ousd.org** unless directed to send elsewhere.

B. Fees for any non-recurring implementation services will be invoiced by Incident IQ on a one-time basis and paid by You upon commencement of the Services Period.

4.2. Payment. You will pay all fees due by **April 5, 2024.** Payment is not dependent upon completion of any implementation or other services.

5. AUTHORIZED ADMINISTRATORS & LEGAL NOTICES

Your contact for order confirmation and system notices are:

Authorized Administrator

Name:**Kyleigh Nevis**

Authorized Administrator Email: **kyleigh.nevis@ousd.org**

All legal notices will be in writing and given when delivered to the address or email address given below.

If to Incident IQ:
Attn: Legal
750 Glenwood Ave SE, Suite 320
Atlanta, GA 30316
legal@incidentiq.com

If to You:
Oakland Unified
1011 Union Street Oakland, CA 94607
Attn: **Kyleigh Nevis**
kyleigh.nevis@ousd.org

The parties understand and agree that day-to-day communications made in the ordinary course of business may be made between others than those referenced above.

The undersigned has the authority to enter into and to bind the respective party to this Agreement as outlined in the Order Form, the accompanying MSA, and all accompanying exhibits contained herein.

For **Oakland Unified**

BY:

Susan Beltz

DATE:

INCIDENT IQ CLOUD SERVICES
MASTER SUBSCRIPTION AGREEMENT (MSA)

Revised January 1, 2023,

Effective January 8, 2023

THIS AGREEMENT GOVERNS YOUR ACQUISITION AND USE OF OUR CLOUD SERVICES.

THE APPLICABLE PROVISIONS OF THIS AGREEMENT ALSO GOVERN ANY PILOT TRIAL. THE TERMS OF THIS AGREEMENT EXPRESSLY SUPERSEDE ALL PRIOR TERMS OF ALL PRIOR AGREEMENTS. **THIS AGREEMENT APPLIES TO ALL AGREEMENTS ENTERED INTO ON AND AFTER JANUARY 8, 2023**; AGREEMENTS PREDATING THIS AGREEMENT SHALL BE GOVERNED BY THE TERMS APPLICABLE AT THE DATE OF EXECUTION.

YOU ACCEPT THE TERMS OF THIS MSA BY EXECUTING AN "ORDER FORM" AND/OR PILOT SERVICE AGREEMENT THAT REFERENCES THIS AGREEMENT. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A SEPARATE LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERMS "YOU" OR "YOUR" SHALL REFER TO SUCH ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE CLOUD SERVICES.

1 DEFINITIONS

1.1 "Acceptable Use Policy" or "AUP" is defined in Section 2.

1.2 "Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity.

1.3 "Agreement" means this Master Subscription Agreement.

1.4 "Cloud Services" means products using Our proprietary cloud service, ("Incident IQ Platform" or "iiQ Platform" or "Platform") and any related offerings, as identified in the relevant Order and as modified from time to time. The Cloud Service includes Our Software and Documentation but not Professional Services deliverables or Third-Party Content.

1.5 "Content" means information obtained by Incident IQ from publicly available sources or third-party content providers and made available to You through the Cloud Services or pursuant to an Order Form.

1.6 "Confidential Information" means information disclosed by or on behalf of one party (as discloser) to the other party (as recipient) under this

Agreement, in any form, which (a) the discloser identifies to recipient as "confidential" or "proprietary" or (b) should be reasonably understood as confidential or proprietary due to its nature and the circumstances of its disclosure. Our Confidential Information includes technical or performance information about the Cloud Service, and Customer's Confidential Information includes Customer Data.

1.7 "Customer" means the party purchasing Cloud Services from Us.

1.8 "Customer Data" means any data, content or materials that Customer (including its Users and any other interested stakeholders) uploads into, enters into, or submits to its Cloud Service accounts, including from Third-Party Platforms. For clarification, Customer Data excludes Usage Data (defined below).

1.9 "Customer Materials" means materials and resources that Customer makes available to Provider in connection with Professional Services.

1.10 "Documentation" means Our standard usage documentation for the Cloud Services.

1.11 "Effective Date" means the first day that Customer has access to the Cloud Services purchased with an Order Form.

1.12 "Feedback" means any information provided by You to Incident IQ regarding an existing or potential future product, service, or other performance provided by or sought from Incident IQ.

1.13 "Force Majeure" means an unforeseen event beyond a party's reasonable control, such as a strike, blockade, war, pandemic, act of terrorism, riot, third-party Internet or utility failure, refusal of government license or natural disaster, where the affected party takes reasonable and customary measures to avoid or mitigate such event's effects.

1.14 "Laws" means all laws, regulations, rules, court orders or other binding requirements of a governmental authority that apply to a party.

1.15 "Order Form" means an ordering document or online order specifying the Cloud Services and related services to be provided by Us under the terms of this Master Subscription Agreement (MSA), including any addenda and supplements thereto. Typically includes a purchase order submitted by You in response to a price quotation ("quote") provided by Us or a third party authorized by Us to resell the Cloud Services. The purchase order and the quote together constitute an "Order Form" for the purposes of any relevant Agreement.

1.16 “Personal Data” means Customer Data relating to an identified or identifiable natural person.

1.17 “Protected Student Information” means “Student Personally Identifiable Information” or “Student Education Records,” within the meaning of the Family Educational Rights and Privacy Act (FERPA) of 1974 and its related provisions under the Code of Federal Regulations, as well as any applicable related state or local laws or regulations

1.18 “Professional Services” means any training, data migration or other professional services that We furnish to You related to the Cloud Services.

1.19 “Renewal” is the process by which the Services Period of certain Cloud Services under an Order Form is extended for an additional Services Period beyond the initial term, unless such Cloud Services are otherwise terminated in accordance with the terms of the Order Form or this Agreement. Your Order Form defines which Cloud Services are eligible for Renewal as well as any terms applicable to any such renewal.

1.20 “Services Period” refers to the period of time for which You ordered the Cloud Services as specified in any Order Form.

1.21 “Statement of Work” means a statement of work for Professional Services that is executed by the parties and references this Agreement.

1.22 “Support” means support provided by Us to Customers for the onboarding and use of the Cloud Services, as governed by the Support Policy.

1.23 “Support Policy” is defined in Support Policy.

1.24 “Suspension Event” means (a) Customer’s account is 30 days or more overdue, (b) Customer is in breach of AUP, and/or (c) Customer’s use of the Cloud Service risks material harm to the Cloud Service or others.

1.25 "Third-Party Claim” means a claim, action, allegation, or other dispute described in Defense & Indemnification brought by a person, entity, or other party that is: (a) not a contracting party to this Agreement or an Order governed by this Agreement; or (b) is an Affiliate of a contracting party to this Agreement (except in the case of a Customer Affiliate that enters into a contract or Order directly with Us and such Order is governed by this Agreement).

1.26 “Third-Party Content” means all text, files, images, graphics, charts, tables, illustrations, information, applications, products, services, data,

audio, video, photographs and other content and material, in any format, that are obtained or derived from third-party sources outside of Incident IQ and made available to You through, within, or in conjunction with Your use of, the Cloud Service.

1.27 "Usage Data" means Our technical logs, data and learnings about Your use of the Cloud Service, including, but not limited to, the number of reports run, the frequency of User log-ins, location of User log-ins, and User behavioral data, such as the types of searches run and features heavily used).

1.28 "User" means those employees, contractors, students, parents, staff, and/or end users, as applicable, authorized by You to use the Cloud Services in accordance with this Agreement and/or Your Order Form.

1.29 "We," "Us" or "Our" means Incident IQ, LLC and its affiliates.

1.30 "You" or "Your" means the legal entity for which you are accepting this Agreement.

2 ACCEPTABLE USE POLICY (AUP):

2.1 You will be responsible for:

2.1.1 Users' compliance with this Agreement and applicable Order Forms,

2.1.2 the accuracy, quality and legality of Your Data and the means by which You acquired Your Data;

2.1.3 using commercially reasonable efforts to prevent unauthorized access to or use of the Cloud Services and Content,

2.1.4 notifying Us promptly of any such unauthorized access or use;

2.1.5 using the Cloud Services and Content only in accordance with this Agreement, Order Forms, and applicable laws and government regulations, including, but not limited to, Children's Online Privacy Protection (COPPA);

2.1.6 complying with terms of service of any Third-Party Content with which You use the Cloud Services.

2.2 You will not:

2.2.1 make the Cloud Services or Content available to, or use the Cloud Services or Content for the benefit of, anyone other than You or authorized Users;

2.2.2 sell, resell, license, sublicense, distribute, make available, rent or lease the Cloud Services or Content;

2.2.3 use the Cloud Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights;

2.2.4 interfere with or disrupt the integrity or performance of the Cloud Services or third-party data contained therein;

2.2.5 attempt to gain unauthorized access to the Cloud Services or Content or its related systems or networks;

2.2.6 permit direct or indirect access to or use of the Cloud Services or Content in a way that circumvents a contractual usage limit, or use any of the Cloud Services to access or use any of Our intellectual property except as permitted under this Agreement or an Order Form;

2.2.7 copy, reverse engineer, or attempt to reverse engineer the Cloud Services or any part, feature, function or user interface thereof;

2.2.8 assist or advise any competitor in their attempts to engineer, reverse engineer, or otherwise copy the Cloud Services or any part, feature, function, or user interface thereof;

2.2.9 copy Content except as permitted by Us in a written agreement;

2.2.10 access the Cloud Services or Content in order to build a competitive product or service or to benchmark with a Non-Incident IQ product or service;

2.2.11 otherwise misuse the Platform in any way contrary with the letter and intent of this Agreement or inconsistent with governing law and/or regulations.

2.2.12 permit users under the age of 13 to use Incident IQ without ensuring all requirements and regulations under COPPA and related state/local regulations are strictly adhered to.

2.3 Any use of the Cloud Services in breach of this Agreement or applicable Order Form by You or Users, that in Our judgment threatens the security, integrity or availability of Our services, may result in immediate suspension of the Cloud Services; however, We will use commercially reasonable efforts under the circumstances to provide You with notice and an opportunity to remedy such violation or threat prior to such suspension.

2.4 You agree to accept all patches, bug fixes, updates, maintenance and service packs (collectively, “Patches”) necessary for the proper function and security of the Cloud Services. Except for emergency or security-related maintenance activities, We will notify You of the scheduling of application of Patches, where possible.

3 INCIDENT IQ RIGHTS AND RESPONSIBILITIES

3.1 We will:

3.1.1 make all commercially reasonable efforts to provide the Cloud Services and Content available to You pursuant to this Agreement and the applicable Order Form;

3.1.2 provide applicable support for the Cloud Services as outlined in our Support Policy at no additional charge following completion of onboarding;

3.1.3 use commercially reasonable efforts to make the online Cloud Services available 24 hours a day, 7 days a week, except for:

3.1.3.1 planned downtime (of which We shall give reasonable advance electronic notice), and

3.1.3.2 any unavailability caused by force majeure.

3.2 We may:

3.2.1 Monitor, observe, compile, store, and/or analyze statistical and other information related to the performance, operation, and use of the Cloud Services;

3.2.2 Utilize Usage Data for security and operations management, to create statistical analyses, and for research and development purposes (clauses 3.2.1 and 3.2.2 are collectively referred to as “Service Analyses”).

3.2.3 We may make Service Analyses publicly available; however, Service Analyses will not incorporate Your Data in a form that could serve to identify You or any individual. We retain all intellectual property rights in Service Analyses.

4 Intellectual Property

4.1 Neither party grants the other any rights or licenses not expressly set out in this Agreement. Except for Our express rights in this Agreement, as between the parties, Customer retains all intellectual property and other rights in Customer Data and Customer Materials provided to Us.

4.2 Except for Customer’s express rights in this Agreement, as between the parties, We retain all intellectual property and other rights in the Cloud

Services, deliverables and related technology (including, but not limited to, all underlying software, source code, design, modules, organization, format, algorithm, and other technology), and all modifications or enhancements thereto and derivatives thereof.

4.3 We may use any Feedback from You or Your Users regarding improvement or operation of the Cloud Services, Support or Professional Services without restriction or obligation.

4.4 Feedback is provided “AS IS” and We will not publicly identify You as the source of feedback without Your permission.

4.5 Unless mutually agreed upon in a separate, fully-executed agreement, We have not agreed to and do not agree to treat as confidential any Feedback You provide to Us, and nothing in this Agreement or in the parties’ dealings arising out of or related to this Agreement will restrict Our right to use, profit from, disclose, publish, keep secret, or otherwise exploit Feedback, without compensating or crediting You. Feedback will not be considered Customer’s Confidential Information, intellectual property, or its trade secret. Once received by Us, such Feedback becomes Our Confidential Information, Intellectual Property, and/or trade secret.

4.6 You grant to Us a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into Our services any feedback suggestion, enhancement request, recommendation, correction or other feedback provided by You or Users relating to the operation of Our services.

5 SAFEGUARDS FOR YOUR DATA.

5.1 Subject to this Agreement, We will access and use Your Data solely to provide and maintain the Cloud Services, Support, and Professional Services under this Agreement. Such use includes sharing Your Data as You direct through the Cloud Services, but We will not otherwise disclose Customer Data to third-parties except as permitted in this Agreement, or otherwise required by law.

5.2 We will implement and maintain reasonable Security Measures that:

5.2.1 Are consistent with all federal, state, and local law and regulations;

5.2.2 Will use appropriate and reasonable technical and organizational measures designed to prevent unauthorized access, use, alteration or disclosure of Customer Data.

5.2.3 Will be audited by an external auditor, at Our expense and no less frequently than annually, to verify the adequacy of Our control measures according to SOC 2 standards and/or such other similar standards that are substantially equivalent to such control standards. Such audit will result in the generation of an audit report;

5.2.3.1 Such audit reports will be deemed Our Confidential Information/

5.2.3.2 Such audit reports may be made available to You upon your request to legal@incidentiq.com and execution of a separate non-disclosure agreement provided by us. This provision does not constitute an entitlement by You to any such audit report.

5.2.3.3 Any release of such audit reports are at our sole discretion. We may provide any reason or no reason at all for deciding to disclose or not disclose an audit report.

5.3 For any of Your Data residing in the Cloud Services environment and identified by You or Your Users or the law as “Protected Student Information,” We will undertake the following measures with respect to such data:

5.3.1 Only collect, process and store such Protected Student Information as is necessary to provide the cloud services under this Agreement;

5.3.2 Under no circumstances will We use such information to market or advertise to students or their family members or legal guardians, or otherwise use such information to inform, influence or enable marketing, advertising or other commercial efforts by a third party directed at students, their family members, or legal guardians;

5.3.3 Shall not change how Protected Student Information is collected, maintained, used or disclosed under the terms of the Agreement, without advance notice to and prior written consent from You.

5.4 Upon notice of a request for a copy of certain Protected Student Information in Our possession from You or a Person authorized under federal, state, and/or local law and regulations, we will ensure that:

5.4.1 A complete and readable digital copy of the requested Protected Student Information in Our possession is delivered to You within 30 days (or the maximum time permitted under law, whichever is greater) of our receipt of Your request;

5.4.2 Upon delivery of the copy to a Person authorized under federal, state, and/or local law and regulations, we will notify You of such disclosure if permitted by law. Such notification will be within the timeframe outlined in 5.4.1 above.

5.4.3 Such notice under 5.4 must be submitted to legal@incidentiq.com to constitute "notice" under section 5.4.

5.5 Upon notice of a request from You that certain Protected Student Information be deleted, we will:

5.5.1 permanently destroy (i.e., undertake a nonrecoverable deletion process in accordance with Department of Defense standard 5220.22-M) all copies of the Protected Student Information identified for deletion by You held by Us or any of Our agents, subcontractors or affiliates; and

5.5.2 Within 30 days of Your notice, we will deliver a written confirmation to You certifying that the permanent destruction of the requested Protected Student Information has been accomplished. Upon delivery of such written confirmation of deletion, you must provide notice to Us of Your receipt and understanding of said notice confirming deletion made at Your request.

5.5.3 Such notice under 5.5 must be submitted to legal@incidentiq.com to constitute "notice" under section 5.5

5.6 Regardless of whether we receive any request, we shall delete or otherwise destroy all of Your Protected Student Information, using the methods described above, following expiration of a 60-day period after termination of this Agreement.

5.7 We will operate the Cloud Services and collect, process and store Protected Student Information 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 Student Information, and prevent unauthorized access, disclosure and use.

5.8 We will never use Protected Student Information that we acquire through Your use of the Cloud Services for any commercial purposes, except as part of a "corporate action" (i.e., purchase, sale, merger, or other type of acquisition), if so permitted by law.

5.8.1 We will notify you if such a “corporate action” occurs. In such a case, we warrant any successor entity shall be contractually obligated to comply with the terms of this Agreement related to the treatment of Protected Student Information, as well as all other applicable legal requirements governing the use, disclosure, and security of the previously acquired Protected Student Information.

5.9 In the event of any security incident (including any actual or suspected data breach) that affects Your Data, we will follow our Information Security Policy. Unless specified in Your Order Form, or otherwise required by law, We will notify you at a time and in a manner consistent with reasonable industry standards if we detect or suspect a security incident affecting Your data occurs.

6 SUBSCRIPTION TERMS

6.1 Unless otherwise provided in the applicable Order Form and/or any other addenda/supplements, each Subscription Term will last for an initial 12-month period.

6.2 Such Agreement starts on the “Effective Date” and continues until the end of the subscription term, unless sooner terminated in accordance with these terms. If no Subscription Term is in effect, either party may terminate this Agreement for any or no reason with notice to the other party.

6.3 Additional offerings and/or subscriptions may be added during a subscription term, and will prorated for the portion of that original subscription term remaining at the time the subscriptions are added. Unless otherwise indicated, any products/services added during a subscription will terminate on the same date as the preceding, underlying subscriptions.

7 FEES & PAYMENTS

7.1 All fees payable to Incident IQ are due within 30 days from the invoice date or as otherwise outlined in the Order Form.

7.2 Late payments are subject to a charge of 1.5% per month, or the maximum amount allowed by Law, whichever is less. All fees and expenses are non-refundable except as expressly set out in this Agreement.

7.3 You will pay any sales, value-added or other similar taxes imposed by applicable law that Incident IQ must pay based on the Cloud Services You ordered, except for taxes based on Incident IQ’s income.

7.4 If You dispute an invoice in good faith, You will notify Us within the Payment Period and the parties will seek to resolve the dispute over a 15-day discussion period. You are not required to pay disputed amounts during the discussion period, but will timely pay all undisputed amounts. After the discussion period, either party may pursue any available remedies.

7.4.1 Any such notification of dispute under 7.4 must be sent to accounting@incidentiq.com.

8 NON-INCIDENT IQ PROVIDERS

8.1 We or third-parties may make available Third-Party Content. Incident IQ does not control and is not responsible for any such Third-Party Content accessible from or provided through the Cloud Services, and You bear all risks associated with any such access and use. Any Third-Party Content made accessible by Incident IQ in or through the Cloud Services is provided on an “as-is” and “as available” basis without any warranty of any kind.

8.2 If You choose to utilize any Third-Party Content, You grant Us permission to allow the relevant provider of such Third-Party Content to access Your Data as required for the interoperation of that Third-Party Content with the Cloud Services. We are not responsible for any disclosure, modification or deletion of Your Data resulting from access by such Third-Party Content or its provider.

9 CONFIDENTIALITY

9.1 By virtue of this Agreement, the parties may have access to information that is confidential to one another (“Confidential Information”). We each agree to disclose only information that is required for the performance of obligations under this Agreement or in order to comply with any governing law or binding court order.

9.2 Confidential information shall be limited to Your Data residing in the Cloud Services, and all information identified as confidential at the time of disclosure.

9.3 A party’s Confidential Information shall not include information that: (a) is or becomes a part of the public domain through no act or omission of the other party; (b) was in the other party’s lawful possession prior to the disclosure and had not been obtained by the other party either directly or indirectly from the disclosing party; (c) is lawfully disclosed to the other party by a third party without restriction on the disclosure; or (d) is independently developed by the other party. Provided, however, Student

Education Records shall never not be deemed Confidential Information.

9.4 We each agree not to disclose each other's Confidential Information to any third-party other than as set forth in the following sentence for a period of three (3) years from the date of the disclosing party's disclosure of the Confidential Information to the receiving party; however, We will hold Your Confidential Information that resides within the Cloud Services in confidence for as long as such information resides in the Cloud Services.

9.4.1 We each may disclose Confidential Information only to those employees, agents or subcontractors who have a demonstrated need to know. Such recipients are required to protect it against unauthorized disclosure in a manner no less protective than required under this Agreement.

9.4.2 Incident IQ will protect the confidentiality of Your Data residing in the Cloud Services in accordance with the Incident IQ security practices defined as part of Your Order Forms.

9.4.3 In addition, Your Data will be treated in accordance with the terms outlined above. Nothing shall prevent either party from disclosing Confidential Information as required by law.

9.5 In performing the Cloud Services, We will comply with the Incident IQ Privacy Policy, (available at https://www.incidentiq.com/privacy-policy) and incorporated herein by reference, as well as any additional requirements contained in applicable Order Forms or other documents.

9.5.1 The Incident IQ Privacy Policy is subject to change at Our discretion; however, policy changes will not result in a material reduction in the level of protection provided for Your Data during the Services Period described in Your Order Form.

9.6 We will maintain industry-standard administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Your Data. Those safeguards will include, but will not be limited to, measures for preventing access, use, modification or disclosure of Your Data by Our personnel except (a) to provide the purchased Cloud Services and prevent or address service or technical problems, (b) as compelled by law, or (c) as You expressly permit in writing.

10 TERMINATION

10.1 In addition to any other remedies it may have, either party may also terminate this Agreement upon thirty (30) days' notice (or without notice in the case of nonpayment), if the other party materially breaches any of the terms or conditions of this Agreement or an applicable Order Form.

10.1.1 In the event we terminate for cause under 10.1 and you have not yet paid, You agree we have the right to immediately collect all sums due from You between the date of termination under 10.1 and the first day of the subscription.

10.1.2 In the event we terminate for cause under 10.1 after payment, we have full discretion on whether we will refund, whether in whole or in part, the balance of any payments made by You between the date of termination under 10.1 and the last day of the subscription.

10.2 We reserve the right to terminate any agreement at any time for any reason, or no reason at all, upon ninety (90) days' notice.

10.2.1 In the event we terminate under 10.2 and you have not yet paid, You agree we have the right to immediately collect all sums due from You between the date of termination following the notice period under 10.2 and the first day of the subscription.

10.2.2 In the event we terminate under 10.2 after payment, we will refund you the balance of any payments made by You between the date of termination and the last day of the subscription.

10.3 You must pay in full for the Cloud Services up to and including the last day on which the Cloud Services are provided.

10.4 All aspects of this Agreement which by their nature should survive termination will survive termination, including, but not limited to, accrued rights to payment, confidentiality obligations, warranty disclaimers, and limitations of liability.

11 WARRANTIES, REMEDIES AND DISCLAIMERS

11.1 Incident IQ warrants that it will make all reasonable efforts to perform the Cloud Services in all material respects as described in Your Order Form. If the Cloud Services provided to You were not performed as warranted, You must promptly provide written notice to Incident IQ that describes the deficiency in the Cloud Services.

11.2 Incident IQ does not guarantee that:

11.2.1 The services will be performed error-free or uninterrupted, or that Incident IQ will correct all services errors;

11.2.2 The services will operate in combination with your content or your applications, or with any other hardware, software, systems or data not provided by Incident IQ, and the Cloud Services will meet your requirements, specifications or expectations. You acknowledge that Incident IQ does not control the transfer of data over communications facilities, including the internet, and that the cloud services may be subject to limitations, delays, and other problems inherent in the use of such communications facilities. Neither party shall be responsible for any delays, delivery failures, or other damage resulting from such problems. Incident IQ is not responsible for any issues related to the performance, operation or security of the cloud services that arise from your data or third-party content;

11.2.3 Any representation or warranty regarding the reliability, accuracy, completeness, correctness, or usefulness of third-party content, and disclaims all liabilities arising from or related to third party content is true.

11.3 For any breach of the Cloud Services warranty, Your exclusive remedy and Incident IQ's entire liability, shall be the correction of the deficient Cloud Services that caused the breach of warranty, or, if Incident IQ cannot substantially correct the deficiency in a commercially reasonable manner, You may end the deficient Cloud Services, and Incident IQ will refund to you the fees for the terminated services that you pre-paid to Incident IQ for the period following the effective date of termination, in a manner consistent with 10.2 above.

11.4 To the extent not prohibited by law, these warranties are exclusive and there are no other express or implied warranties or conditions including for software, hardware, systems, networks or environments or for merchantability, satisfactory quality and fitness for a particular purpose.

12 LIMITATION OF LIABILITY

12.1 To the maximum extent permitted by law, each party's entire liability arising out of or related to this Agreement will not exceed the amounts paid or payable by You to US under this Agreement immediately preceding the first incident giving rise to liability."

12.2 Neither party will have any liability arising out of or related to this Agreement for indirect, special, incidental, reliance or consequential damages or damages for loss of use, lost profits or interruption of operations, even if informed of their possibility in advance.

12.3 The waivers and limitations in this Section apply regardless of the form of

action, whether in contract, tort (including negligence), strict liability or otherwise and will survive and apply even if any limited remedy in this Agreement fails of its essential purpose.

13 DEFENSE & INDEMNIFICATION

13.1 We will defend You and Your employees and trustees (hereinafter and for purposes of this Section, collectively referred to as “You”) against any claim, demand, suit or proceeding made or brought against You by a third-party alleging that the Cloud Services infringe or misappropriate such third-party’s intellectual property rights (a “Claim Against You”), and will indemnify and hold harmless You from any damages, attorney fees and costs ultimately awarded against You as a result of, or for amounts paid by You under a settlement approved by Us in writing of, a Claim Against You.

13.1.1 In order to receive the benefit of this indemnification, you must:

13.1.1.1 promptly give Us written notice of the Claim Against You via email to legal@incidentiq.com;

13.1.1.2 give Us sole control of the defense and settlement of the Claim Against You (except that We may not settle any Claim Against You unless it unconditionally releases You of all liability); and

13.1.1.3 give Us all reasonable assistance.

13.1.2 If We receive information about an infringement or misappropriation claim related to the Cloud Services, We shall, in Our discretion and at no cost to You:

13.1.2.1 modify the Cloud Services so that they are no longer claimed to infringe or misappropriate, without breaching Our warranties described above; or

13.1.2.2 obtain a license for Your continued use of that Service in accordance with this Agreement; or

13.1.2.3 terminate Your subscriptions for the Cloud Services upon 30 days' written notice and refund You any prepaid fees covering the remainder of the term of the terminated subscriptions, consistent with 10.2 above.

13.1.3 The above defense and indemnification obligations do not apply to the extent a Claim Against You arises from Content, Third-Party Content or Your use of the Cloud Services in violation of this Agreement or applicable Order Forms; provided such Claim Against You would not have arisen but for Your use in violation of this Agreement or applicable Order Forms.

13.2 **Unless otherwise prohibited by state law and/or local regulations**, You will defend and indemnify Us against any claim, demand, suit or proceeding made or brought against Us by a third-party alleging that any of Your Data infringe or misappropriate such third-party's intellectual property rights, or arising from Your use of the Cloud Services or Content in violation of the Agreement, Order Forms or applicable law (each a "Claim Against Us"), and You will indemnify Us from any damages, attorney fees and costs ultimately awarded against Us as a result of, or for any amounts paid by Us under a settlement approved by You in writing of, a Claim Against Us, provided We (a) promptly give You written notice of the Claim Against Us, (b) give You sole control of the defense and settlement of the Claim Against Us (except that You may not settle any Claim Against Us unless it unconditionally releases Us of all liability), and (c) give You all reasonable assistance, at Your expense.

13.3 This Section states the indemnifying party's sole liability to, and the

indemnified party's exclusive remedy against, the other party for any type of claim described in this Section.

14 MISCELLANEOUS PROVISIONS

14.1 Severability. If any provision of this Agreement is held to be invalid or unenforceable, the invalidity or unenforceability will not affect the other provisions of the Agreement.

14.2 No Waiver. A waiver of any breach of this Agreement is not deemed a waiver of any other breach.

14.3 Notices. All notices will be in writing, transmitted via certified or registered mail, postage prepaid, and delivered to the address set forth in Your Order Form. Notices may also be transmitted via e-mail and delivered to the addresses set forth in the Order Form. Notices from You to Incident IQ sent via email must be sent to legal@incidentiq.com to constitute proper notification.

14.4 Force Majeure. Neither party is liable for a delay or failure to perform this Agreement due to a Force Majeure. If a Force Majeure materially adversely affects the Cloud Service for 15 or more consecutive days, either party may terminate the affected Order(s) upon notice to the other and Provider will refund to Customer any pre-paid, unused fees for the terminated portion of the Subscription Term. However, this Section does not limit Customer's obligations to pay fees owed.

14.5 Assignment. Neither party may, without the prior written consent of the other party, assign or transfer this Agreement (or any of its rights or obligations) to any other party, except We may assign Our interests as required under any potential corporate action (i.e., acquisition, sale, merger, etc.). In the event of such a corporate action, We warrant that any successor entity will agree to abide by the terms of this agreement for the remainder of any applicable subscription term.

14.6 Relationship of the Parties. The parties are independent contractors, and no partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties is created by this Agreement.

14.7 No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement. For clarification, even though an employee of an Affiliate may be a User under this Agreement, an Affiliate may not bring a claim against Provider arising from, based on, or under this Agreement unless such Affiliate has entered into its own Order directly with Provider.

14.8 Governing Law. **Unless prohibited by state law and/or local regulation**, this Agreement and any claims relating to its subject matter will be governed by and construed under the laws of the State of Georgia, without reference to its conflicts of law principles. All disputes will be subject to the exclusive jurisdiction of the courts located in Fulton County, Georgia or the Federal Court of the Northern District of Georgia. Either party must initiate a cause of action for any claim(s) relating to this Agreement and its subject matter within one year from the date when the party knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

14.9 Entire Agreement. This Agreement and the information which is incorporated into this Agreement by written reference (including reference to information contained in a uniform resource locator or referenced policy), together with the applicable Order Form and accompanying Exhibits, is the complete agreement for the Cloud Services ordered by You and supersedes all prior or contemporaneous agreements or representations, written or oral, regarding such Cloud Services.

SUPPORT POLICY FOR CLOUD SERVICES

1. INTRODUCTION

This Support Policy for Cloud Services ("Policy") sets forth the Support Services identified in Your applicable Order Form. The Services are governed by and subject to the terms and conditions specified in the Master Subscription Agreement and applicable Order Form signed by You (collectively the "Agreement").

2. Support Tiers

2.1. Tier One Support for Users.

2.1.1. Incident IQ Help Center. All of Your Users may access to written help documentation and video tutorials via the Cloud Services help center (located at https://help.incidentiq.com and through Incident IQ Academy at learn.incidentiq.com.

2.1.2. Support Request within Cloud Services Environment. All of Your Users may submit an "Incident IQ Help Ticket" using the Cloud Services. These requests first route to Your Administrator Users for resolution. If necessary Your Administrator Users may forward the request within the Cloud Services environment to the Incident IQ product support team.

2.2 Tier Two Support for Users.

2.2.1 Your Administrator Users can escalate other User help requests within the Cloud Services to the Cloud Services product support team or make such requests to the product support team directly.

2.2.2 Your Administrator Users also may access toll-free telephone support (866-899-9169) and email support (support@incidentiq.com) from the product support team during ordinary business hours (Monday through Friday, 8AM to 8PM Eastern Standard Time, excluding holidays).

3. Response Time Service Level

The Cloud Services product support team will strive to respond to support requests from Your Administrator Users within one (1) business day.