

Appendix A

Compliance With New York State Education Law Section 2-d Addendum ("Addendum")

The parties to this Agreement are the Monroe 1 Board of Cooperative Educational Services ("BOCES") and CLPS, LLC. ("Vendor"). BOCES is an educational agency, as that term is used in Section 2-d of the New York State Education Law ("Section 2-d") and its implementing regulations, and Vendor is a third-party contractor, as that term is used in Section 2-d and its implementing regulations. BOCES and Vendor have entered into this Agreement to conform to the requirements of Section 2-d and its implementing regulations. To the extent that any term of any other agreement or document conflicts with the terms of this Agreement, the terms of this Agreement shall apply and be given effect.

Definitions

As used in this Agreement and related documents, the following terms shall have the following meanings: "Student Data" means personally identifiable information from student records that Vendor receives from an educational agency (including BOCES or a Participating School District) in connection with providing Services under this Agreement.

"Personally Identifiable Information" ("PII") as applied to Student Data, means personally identifiable information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA), at 20 USC 1232g.

"Third Party Contractor," "Contractor" or "Vendor" means any person or entity, other than an educational agency, that receives Student Data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to such educational agency, including, but not limited to data management or storage services, conducting studies for or on behalf of such educational agency, or audit or evaluation of publicly funded programs.

"BOCES" means Monroe #1 Board of Cooperative Educational Services.

"Parent" means a parent, legal guardian, or person in parental relation to a student.

"Student" means any person attending or seeking to enroll in an educational agency.

"Eligible Student" means a student eighteen years or older.

"State-protected Data" means Student Data, as applicable to Vendor's product/service.

"Participating School District" means a public school district or board of cooperative educational services that obtains access to Vendor's product/service through a cooperative educational services agreement ("CoSer") with BOCES, or other entity that obtains access to Vendor's product/service through an agreement with BOCES, and also includes BOCES when it uses the Vendor's product/service to support its own educational programs or operations.

"Breach" means the unauthorized access, use, or disclosure of personally identifiable information.

"Commercial or marketing purpose" means the sale of PII; and the direct or indirect use or disclosure of State-protected Data to derive a profit, advertise, or develop, improve, or market products or services to students other than as may be expressly authorized by the parties in writing (the "Services").

"Disclose", "Disclosure," and "Release" mean to intentionally or unintentionally permit access to State-protected Data; and to intentionally or unintentionally release, transfer, or otherwise communicate State-protected Data to someone not authorized by contract, consent, or law to receive that State-protected Data.

Vendor Obligations and Agreements

Vendor agrees that it shall comply with the following obligations with respect to any student data received in connection with providing Services under this Agreement and any failure to fulfill one of these statutory or regulatory obligations shall be a breach of this Agreement. Vendor shall:

(a) limit internal access to education records only to those employees and subcontractors that are determined to have legitimate educational interests in accessing the data within the meaning of Section 2-d, its implementing regulations and FERPA (e.g., the individual needs access in order to fulfill his/her responsibilities in providing the contracted services);

(b) only use personally identifiable information for the explicit purpose authorized by the Agreement, and must/will not use it for any purpose other than that explicitly authorized in the Agreement or by the parties in writing;

(c) not disclose any personally identifiable information received from BOCES or a Participating School District to any other party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Agreement, unless (i) if student PII, the Vendor or that other party has obtained the prior written consent of the parent or eligible student, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to the source of the information no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

(d) maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of the personally identifiable information in its custody;

(e) use encryption technology to protect data while in motion or in its custody (i.e., in rest) from unauthorized disclosure by rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States department of health and human services in guidance issued under Section 13402(H)(2) of Public Law 111-5 using a technology or methodology specified or permitted by the secretary of the U.S.);

(f) not sell personally identifiable information received from BOCES or a Participating School District nor use or disclose it for any marketing or commercial purpose unless otherwise expressly authorized by the Services, or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

(g) notify the educational agency from which student data is received of any breach of security resulting in an unauthorized release of such data by Vendor or its assignees in violation of state or federal law, or of contractual obligations relating to data privacy and security in the most expedient way possible and without unreasonable delay, in compliance with New York law and regulation;

(h) reasonably cooperate with educational agencies and law enforcement to protect the integrity of investigations into any breach or unauthorized release of personally identifiable information by Vendor;

(i) adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework, Version 1.1, that are in substantial compliance with the BOCES data security and privacy policy, and that comply with Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth below, as well as all applicable federal, state and local laws, rules and regulations;

(j) acknowledge and hereby agrees that the State-protected Data which Vendor receives or has access to pursuant to this Agreement may originate from several Participating School Districts located across New York State. Vendor acknowledges that the State-protected Data belongs to and is owned by the Participating School District or student from which it originates;

(k) acknowledge and hereby agrees that if Vendor has an online terms of service and/or Privacy Policy that may be applicable to its customers or users of its product/service, to the extent that any term of such online terms of service or Privacy Policy conflicts with applicable law or regulation, the terms of the applicable law or regulation shall apply;

(l) acknowledge and hereby agrees that Vendor shall promptly pay for or reimburse the educational agency for the full third party cost of a legally required breach notification to parents and eligible students due to the unauthorized release of student data caused by Vendor or its agent or assignee;

(m) ensure that employees, assignees and agents of Contractor 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 to such data; and

(n) ensure that any subcontractor that performs Contractor's obligations pursuant to the Agreement is legally bound by legally compliant data protection obligations imposed on the Contractor by law, the Agreement and this Agreement.

Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security

()

The Monroe #1 BOCES seeks to use current technology, including electronic storage, retrieval, and analysis of information about students' education experience in the BOCES, to enhance the opportunities for learning and to increase the efficiency of our operations.

The Monroe #1 BOCES seeks to ensure that parents have information about how the BOCES stores, retrieves, and uses information about students, and to meet all legal requirements for maintaining the privacy and security of protected student data and protected principal and teacher data, including Section 2-d of the New York State Education Law.

To further these goals, the BOCES has posted this Parents' Bill of Rights for Data Privacy and Security.

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education record. The procedures for exercising this right can be found in Student Records Policy 6320.
()
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by the State is available at
and a copy may be

obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

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

Chief Privacy Officer
New York State Education Department
Room 863 EBA
89 Washington Avenue
Albany, New York 12234.

or

Monroe One Data Protection Officer
William Gregory
Monroe #1 BOCES
41 O'Connor Road
Fairport, NY 14450

Supplemental Information About Agreement Between COMPANY and BOCES

(a) The exclusive purposes for which the personally identifiable information provided by BOCES or a Participating School District will be used by Vendor is to provide COMPANY's school safety services and solutions to BOCES or other Participating School District pursuant to a BOCES Purchase Order.

(b) Personally identifiable information received by Vendor, or by any assignee of Vendor, from BOCES or from a Participating School District shall not be sold or used for marketing purposes.

(c) Personally identifiable information received by Vendor, or by any assignee of Vendor shall not be shared with a sub-contractor except pursuant to a written contract that binds such a party to at least the same data protection and security requirements imposed on Vendor under this Agreement, as well as all applicable state and federal laws and regulations.

(d) The effective date of this Agreement shall be July 31, 2023, and the Agreement shall remain in effect until July 31, 2025, unless sooner by either party for any reason upon thirty (30) days' notice.

(e) Upon expiration or termination of the Agreement without a successor or renewal agreement in place, and upon request from BOCES or a Participating School District, Vendor shall transfer all educational agency data to the educational agency in a format agreed upon by the parties. Vendor shall thereafter securely delete all educational agency data remaining in the possession of Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies) as well as any and all educational agency data maintained on behalf of Vendor in secure data center facilities, other than any data that Vendor is required to maintain pursuant to law, regulation or audit requirements. Vendor shall ensure that no copy, summary or extract of the educational agency data or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the secure data center facilities unless Vendor is required to keep such data for legal, regulator, or audit purposes, in which case the data will be retained in compliance

with the terms of this Agreement. To the extent that Vendor and/or its subcontractors or assignees may continue to be in possession of any de-identified data (data that has had all direct and indirect identifiers permanently removed with no possibility of reidentification), they each agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to the BOCES or Participating School District from an appropriate officer that the requirements of this paragraph have been satisfied in full.

(f) State and federal laws require educational agencies to establish processes for a parent or eligible student to challenge the accuracy of their student data. Third party contractors must cooperate with educational agencies in complying with the law. If a parent or eligible student submits a challenge to the accuracy of student data to the student's district of enrollment and the challenge is upheld, Vendor will cooperate with the educational agency to amend such data.

(g) Vendor shall store and maintain PII in electronic format on systems maintained by Vendor in a secure data center facility in the United States in accordance with its Privacy Policy, NIST Cybersecurity Framework, Version 1.1, and the BOCES data security and privacy policy, Education Law Section 2-d, Part 121 of the Regulations of the Commissioner of Education, and the Monroe #1 BOCES Parents' Bill of Rights for Data Privacy and Security, set forth above. Encryption technology will be utilized while data is in motion and at rest, as detailed above.

(h) A copy of Vendor's Data Privacy and Security Plan, which vender affirms complies with 8 N.Y.C.R.R. 121.6 is attached hereto as **Attachment 1** and is incorporated herein by reference as if fully set forth herein.



Vendor Signature

July 31, 2023

ATTACHMENT 1 - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Data is only accessible to accounts that the data is associated with. All Personal Identifiable Information is encrypted. Data is deleted once it is no longer needed.
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	PII information is encrypted in the database. The key is only given in emergency situations.
3	Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.	All employees are trained on Cybersecurity practices including phishing attacks.
4	Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	Contracts include language to follow CLPS security protocols and privacy policies.
5	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.	In the case of a data breach the account administrators are notified. The security hole is immediately investigated at as top priority.
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon completion of the contractual obligation, the account can download their data on the website or request any custom reports while the data is still in the system.
7	Describe your secure destruction practices and how certification will be provided to the EA.	Data is removed from the database after a retention period. Archived

		data and backups remain for a longer retention period.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	The EA is concerned about data privacy particularly around PII. CLPS has additional encryption regarding this data.
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	PLEASE USE TEMPLATE BELOW.

ATTACHMENT 1(A) – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at <https://www.nist.gov/cyberframework/new-framework>. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	User's computers are file encrypted. All account data is kept in an online infrastructure behind a strong password.
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Cybersecurity roles and responsibilities are well defined along with risk management decisions and security protocols.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	All policies and procedures are followed to manage cybersecurity risk.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational	The cybersecurity risk is understood.

Function	Category	Contractor Response
	operations (including mission, functions, image, or reputation), organizational assets, and individuals.	
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Security risk is top priority.
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	CLPS has set protocols for managing and handling security risk and vulnerabilities.
PROTECT (PR)	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	CLPS data is contained in Cloud infrastructure.
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	CLPS is trained on Cybersecurity and phishing attacks.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Data is categorized and given additional levels of encryption when required.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Security and Privacy policies are reviewed.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Yes
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and	Software is upgraded regularly and cybersecurity is kept top of mind.

Function	Category	Contractor Response
	assets, consistent with related policies, procedures, and agreements.	
DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	Activity is detected and reported on.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	The software is monitored for cybersecurity events and is of high priority.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	Activity is detected and alerted on
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	The Response process is well defined and executed on in the case of a data breach.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	The response is coordinated with external stakeholders if necessary.
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Security holes are responded to with urgency and fixes are rolled out as soon as possible
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	The first task to a security incident is to remove access if possible to limit impact.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Upon review of the security incident, lessons are documented and a review of the process and policies are conducted to be updated.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Backups are restored if necessary.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Policies and process are updated upon review of a security incident.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Restoration is conducted with parties necessary.



Security Emergency Management Communication Solution

The easy-to-use cloud-based platform includes a comprehensive A-Z emergency management and communication app specifically built for school environments. The app allows school leaders to collaborate internally with key school decision-makers and externally with emergency responders and other community stakeholder groups. The emergency management and reunification planning features provide school leaders, end-users, and authorized system admins the ability to customize emergency management and reunification plans. The proprietary system includes essential sections, such as functional annexes, threat-specific annexes, active shooter protocol, continuity of operations procedures, school safety teams, student reunification, and threat management. Other unique features include automated safety drill reminders and logging, customized digital safety policies, self-assessment auditing tools, and the capability to upload documents, images, maps, floor plans, and other critical information. The hazard and threat management communication features provide school leaders, end-users, and authorized system admins with the ability to communicate during emergencies instantly and effectively in real-time from classroom computers, laptops, smart phones, and other mobile devices. The system includes reliable connection to law enforcement and satisfies Alyssa's Law requirements in all states. It integrates with other critical software currently being used by schools, including Google Single Sign-on, Active Directory, Informa Cast-Single Wire, Mutualink, Rise Vision, School Tool, and fourDscope. The app can be triggered by wall-mounted panic buttons, soft panic buttons on mobile devices and computers, and other triggering devices. Students can be reunited to their parents, caregivers, or other authorized guardians remotely during emergencies with the app. It is made available to local E911 Dispatch Centers and Law Enforcement at no cost.



Security & Vulnerability Assessment Solution

The easy-to-use cloud-based platform includes a comprehensive A-Z security audit and vulnerability assessment app specifically built for school environments. The app allows school leaders to collaborate internally with keys school decision-makers and externally with emergency responders and other community stakeholder groups. The security auditing and vulnerability assessment features provide school leaders, end-users, and authorized system admins the ability to perform comprehensive security audits and vulnerability assessments at their schools, buildings, facilities, and campuses. The proprietary system uses a quantitative algorithm and analyzes qualitative data to determine risk-level related to emergency planning capabilities, physical security, policies and procedures, emergency communications, and other safety and security related factors. Comprehensive reports detail strengths and provide decision-makers with practical recommendations for school safety improvements. Digital reports are securely archived but can be accessed by authorized managers for revisions and updates on a continuous basis.



Emergency Management & Reunification Plan Solution

The easy-to-use cloud-based platform includes a comprehensive A-Z emergency management and reunification app specifically built for school environments. The app allows school leaders to collaborate internally with key school decision-makers and externally with emergency responders and other community stakeholder groups. The unique features provide school leaders, end-users, and authorized system admins the ability to customize emergency management and reunification plans. The proprietary system includes essential sections, such as functional annexes, threat-specific annexes, active shooter protocol, continuity of operations procedures, school safety teams, student reunification, and threat management. Other unique features include automated safety drill reminders and logging, customized digital safety policies, self-assessment auditing tools, and the capability to upload documents, images, maps, floor plans, and other critical information.



Threat & Behavioral Assessment Solution

The easy-to-use cloud-based platform includes a comprehensive A-Z threat and behavioral assessment app specifically built for school environments. The app allows school leaders to collaborate internally with key school decision-makers and externally with emergency responders and other community stakeholder groups. School leaders and authorized system admins have the ability to set-up school threat assessment teams and perform behavioral assessments on subjects-of-concern, such as students, employees, and other individuals exhibiting threatening behaviors. The proprietary system uses a quantitative algorithm and analyzes qualitative data to determine apparent threat-level of the subject-of-concern. The system is based on research related to the Comprehensive School Threat Assessment Guidelines (CSTAG), Columbia Suicide-Severity Rating Scale, FBI, and U.S. Secret Service. Threat team members have access to CLPS Assessment tools that address Bullying, Harassment, Self-Harm, Suicide, Target Violence, Insider Threats, Outsider Threats, and Title IX cases. Reports are securely stored but can be accessed by authorized school admins for revisions and updates. The system allows for data analytics and the ability to develop customized individual threat management safety plans for ongoing intervention.



Student Reporting Solution

It is critical that students have a viable means to report risky or threatening behaviors to trusted school officials. In 2016, Dr. Matthew Miraglia conducted action-research by having focus groups with over 100 students. For the study, the students were advised that TAP App was considering developing a student reporting app to address violence and other safety-related issues that impact schools. Based on the information provided by these students, the company developed TAP App Student, a cutting-edge student reporting safety app, *"built by student for students."* TAP App Student is an easy-to-use application, that works on iOS, Android, Windows, Chrome, and Mac. It is recommended for 5th graders and above and should be part of every school's threat assessment program.



Digital Training Solution

The easy-to-use cloud-based platform includes a comprehensive A-Z emergency training app specifically built for school environments. The app allows school leaders to deliver essential school safety training to teachers and staff. The proprietary system includes research-based training based on current best practices. Schools can select any of the following courses:

- Active Shooter Preparedness
- Behavioral Threat Assessment
- Bullying Intervention
- Critical Incident Management
- Identifying Suspected Child Abuse
- Student Reunification

Digital certificates of completion are securely archived in the system. Authorized managers have access to real-time progress reports to maintain accountability and ensure legal compliance.



Security Consulting & Training Services

Our company was originally formed as a consulting firm. We have been providing our clients professional risk management, security, and safety consulting services since 2006. Our team of highly credentialed consultants are committed to working with your school's leaders to create and maintain safer and more secure learning environments. Professional consulting and training services include:

- Security/Vulnerability Assessments (Audits)
- Emergency Management Plan Development
- School Safety Policies Development
- Active Shooter Preparedness Training
- Threat & Behavioral Assessment Team Training
- Developing Legally Protective Threat Management Systems for Schools
- Defuse and Manage Confrontational Parents and Challenging Students
- Understanding and Navigating FERPA: A Strategic Roadmap for Schools
- Disaster & Emergency Preparedness Training
- Legal Aspects of Crisis Preparedness and Response
- Situational Awareness Training for Schools
- Stop the Bleed Training (Basic)
- School Safety Project Management
- Mental Health First Aid Training
- Tabletop Exercises



fourDscape

An innovative operating platform for optimal emergency communication and critical incident management

TAP App fourDscape is the most comprehensive hazard and threat management communication system on the market. Every aspect of responding to and managing a critical incident can be accomplished with this cutting-edge platform. The system combines TAP App Emergency Management Communication Solution with fourDscape technology allowing for optimized security systems integration. Within seconds, the system provides on-demand video, voice, and security intelligence systems activation. This allows first responders to respond faster and mitigate incidents more effectively, while collaborating with end-users at the school. With TAP App fourDscape, all systems work together to protect and preserve life. Benefits of this system include:

Immediate Emergency Notification

- Automated lockdown announcement over PA system
- Emergency strobe lights and digital signs activation
- Notifications sent to mobile devices, computers, text, and email
- Police simultaneously notified of emergency
- Triggers existing mass notification systems

Remote Access to Security Systems

- Real-time announcements over PA system
- Live CCTV viewing into building and property
- Doors can be locked and unlocked
- Swipe card system can be deactivated
- Instant viewing of electronic maps and floor plans

Real-Time Incident Management

- Communicate fluidly internally and with first responders
- Emergency procedures can be accessed during an incident
- In-care person accountability
- Push-to-Talk and Instant Messaging
- Emergency Reunification

If security systems already exist at the school (CCTV, Panic Buttons, Automated Locking Systems, Swipe Card Systems, etc.), TAP App fourDscape can integrate everything together. If your school would like to install additional physical security hardware or software, we can do that for you as well!

When seconds matter, the police are only minutes away. With TAP App fourDscape, police response time will be significantly improved so emergency incidents can be resolved faster.

Pricing Schedule

TAP App Security Emergency Management Communication Solution

1 school: \$2,900

More than 1 school: \$1,800 per school.

TAP App Security & Vulnerability Assessment Solution

1 school: \$2,500

More than 1 school: \$1,500 per school.

TAP App Emergency Management & Reunification Plan Solution

1 school: \$2,500

More than 1 school: \$1,500 per school.

TAP App Threat & Behavioral Assessment Solution

1 school: \$2,500

More than 1 school: \$1,500 per school.

TAP App Student Reporting Solution

1 school: \$1,500

More than 1 school: \$1,000 per school.

TAP App Digital Training Solution (Courses: *Active Shooter Preparedness, Behavioral Threat Assessment, Bullying Intervention, Critical Incident Management, Identifying Suspected Child Abuse, Emergency Reunification*): \$500 per course per school.

School Safety Program for New York Schools. Includes TAP App Security Emergency Management Communication, TAP App Student Reporting, TAP App Emergency Management & Reunification Plan, TAP App Threat & Behavioral Assessment, and TAP App Critical Incident Management Digital Course. \$4,950 per school per year (\$3,950 for Utica National Policyholders).

TAP App fourDscape - Base product includes VMS, Doors, and PA system integration with School Safety Program for New York Schools, and current automatic lockdown system if applicable.

1-4 campuses: \$30,000 initial set-up fee, plus \$9,950 or \$8,950 subscription fee per school.

Second year, and thereafter, \$9,950 or \$8,950 subscription fee per school per year.

5 campuses: \$20,000 initial set-up fee, plus \$9,950 or \$8,950 subscription fee per school.

Second year, and thereafter, \$9,950 or \$8,950 subscription fee per school per year.

6 campuses: \$16,667 initial set-up fee, plus \$9,950 or \$8,950 subscription fee per school.

Second year, and thereafter, \$9,950 or \$8,950 subscription fee per school per year.

7 campuses: \$14,286 initial set-up fee, plus \$9,950 or \$8,950 subscription fee per school.

Second year, and thereafter, \$9,950 or \$8,950 subscription fee per school per year.

8 campuses: \$12,500 initial set-up fee, plus \$9,950 or \$8,950 subscription fee per school.

Second year, and thereafter, \$9,950 or \$8,950 subscription fee per school per year.

9 campuses: \$11,111 initial set-up fee, plus \$9,950 or \$8,950 subscription fee per school.

Second year, and thereafter, \$9,950 or \$8,950 subscription fee per school per year.

10 or more campuses: \$10,000 initial set-up fee, plus \$9,950 or \$8,950 subscription fee per school.

Second year, and thereafter, \$9,950 or \$8,950 subscription fee per school per year.

TAP App Security Consulting & Training Services

Security/Vulnerability Assessments (Audits): \$5,000 per school

Emergency Management Plan Development: \$3,000 per school

School Safety Policies Development: \$3,000 per school/district

Active Shooter Preparedness Training: \$2,500 in-person / \$1,500 virtual

Threat & Behavioral Assessment Team Training: \$2,500 in-person / \$1,500 virtual

Developing Legally Protective Threat Management Systems for Schools: \$2,500 in-person / \$1,500 virtual

Defuse and Manage Confrontational Parents and Challenging Students: \$2,500 in-person / \$1,500 virtual

Understanding and Navigating FERPA: A Strategic Roadmap for Schools: \$2,500 in-person / \$1,500 virtual

Disaster & Emergency Preparedness Training: \$2,500 in-person / \$1,500 virtual

Legal Aspects of Crisis Preparedness and Response: \$2,500 in-person / \$1,500 virtual

Situational Awareness Training for Schools: \$2,500 in-person / \$1,500 virtual

Stop the Bleed Training (Basic): \$125 per person; 30-person minimum (not to exceed 75 people)

School Safety Project Management: TBD, contact our office.

Mental Health First Aid Training: TBD, contact our office.

Tabletop Exercises: TBD, contact our office.

**Above consulting and training fees include all travel-related expenses*

TAP App Security - Global Communication system installed at E911 Centers, Police Departments, and Security Incident Command Centers at no additional cost.



800 Corporate Drive, Suite 700

Fort Lauderdale FL 33334

954.361.6152

[CONTACT | clpsconsultants](#)

PRIVACY POLICY

Effective date: June 18, 2019

CLPS, LLC. ("CLPS," "us", "we", or "our") operates the www.clpsconsultants.com website and related applications including the CLPS Suite of Emergency Management Software Solutions, TAP App Security, TAP App Student, and TAP App Wellness mobile applications (collectively, the "Services").

This page informs you of our policies regarding the collection, use, and disclosure of personal data when you use our Services and the choices you have associated with that data.

We use your data to provide and improve the Service. By using the Service, you agree to the collection and use of information in accordance with this policy. Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms and Conditions.

BY INSTALLING, USING, REGISTERING TO OR OTHERWISE ACCESSING ANY SERVICES, YOU AGREE TO THIS PRIVACY POLICY AND GIVE AN EXPLICIT AND INFORMED CONSENT TO THE COLLECTION, USE AND PROCESSING OF YOUR PERSONAL DATA IN ACCORDANCE WITH THIS PRIVACY POLICY. IF YOU DO NOT AGREE TO THIS PRIVACY POLICY, PLEASE DO NOT VISIT, INSTALL, USE, REGISTER TO OR OTHERWISE ACCESS ANY SERVICES.

Definitions

Service

Services means the www.clpsconsultants.com website and related software solution and applications.

Personal Data

Personal Data means data about a living individual who can be identified from those data (or from those and other information either in our possession or likely to come into our possession).

Usage Data

Usage Data is data collected automatically either generated by the use of the Services or from the Services infrastructure itself (for example, the duration of a page visit).

Cookies

Cookies are small pieces of data stored on your device (computer or mobile device).

Data Controller

Data Controller means the natural or legal person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal information are, or are to be, processed.

For the purpose of this Privacy Policy, we are a Data Controller of your Personal Data.

Data Processors (or Service Providers)

Data Processor (or Service Provider) means any natural or legal person who processes the data on behalf of the Data Controller.

We may use the services of various Service Providers in order to process your data more effectively.

Data Subject (or User)

Data Subject is any living individual who is using our Services and is the subject of Personal Data.

Information Collection And Use

We collect several different types of information for various purposes to provide and improve our service to you.

Types of Data Collected

Personal Data

While using our Service, we may ask you to provide us with, or your school or employer may have provided us with, certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personal Data may include, but is not limited to:

- Email address
- First name and last name
- Phone number
- Address, State, Province, ZIP/Postal code, City
- Cookies and Usage Data
- Job Title or Role
- Class or school enrollment or attendance

We may use your Personal Data to contact you with newsletters, marketing or promotional materials and other information that may be of interest to you. You may opt out of receiving any, or all, of these communications from us by following the unsubscribe link or instructions provided in any email we send.

Usage Data

We may also collect information that your browser sends whenever you visit our Services or when you access the Services by or through a mobile device ("Usage Data").

This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Services that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When you access the Services by or through a mobile device, this Usage Data may include information such as the type of mobile device you use, your mobile device unique ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browser you use, unique device identifiers and other diagnostic data.

Tracking Cookies Data

We use cookies and similar tracking technologies to track the activity on our Services and hold certain information.

Cookies are files with small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyze our Service.

You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

Examples of Cookies we use:

- **Session Cookies.** We use Session Cookies to operate our Service.
- **Preference Cookies.** We use Preference Cookies to remember your preferences and various settings.
- **Security Cookies.** We use Security Cookies for security purposes.
- **Advertising Cookies.** Advertising Cookies are used to serve you with advertisements that may be relevant to you and your interests.

Mobile Data

We use mobile analytics software to allow us to better understand the functionality of our mobile application on your phone. This software may record information such as how often you use the application, the events that occur within the application, aggregated usage, performance data, and where the application was downloaded from. We do not link the information we store within the analytics software to any personally identifiable information you submit within the mobile application.

We may send you push notifications from time-to-time in order to update you about any events or promotions that we may be running. The mobile application may also ask for your permission to access your camera and your photos. If you no longer wish to receive these types of communications, or if you've initially agreed for the application to access your camera and photos and you would like to stop the app from accessing them, you may turn them off at the device level. To ensure you receive proper notifications, we will need to collect certain information about your device such as operating system and user identification information.

We do not ask for, access or track any location-based (precise location) information from your mobile device at any time while downloading or using our Mobile Apps or Services.

Use of Data

CLPS, LLC uses the collected data for various purposes, including, but not limited to:

- To provide and maintain our Service
- To provide and transmit data to emergency responders, safety, or school officials, or, if applicable, your employer

- To administer your account
- To notify you about changes to our Services
- To allow you to participate in interactive features of our Services when you choose to do so
- To provide customer support
- To provide you with access to particular tools or features
- To respond to your inquiries and send you administrative communications
- To gather analysis or valuable information so that we can improve our Service
- To monitor the usage of our Service
- Obtain your feedback on our sites and our offerings
- Conduct research and measurement activities
- To detect, prevent and address technical issues
- To provide you with news, special offers and general information about other goods, services and events which we offer that are similar to those that you have already purchased or enquired about unless you have opted not to receive such information

We may combine information that we collect about you with information from external sources. We may use this information to provide services to you such as personalized content.

To enhance our services, we may share your information with any member of our group of companies (this means our subsidiaries, parent and affiliated companies) as well as with third parties who provide services on our behalf to help with our business activities such as email service providers, data analyzers and business intelligence providers for the purpose of enhancing or maintaining the Software, our products and services. These companies are authorized to use your personal information only as necessary to provide these services to us.

Legal Basis for Processing Personal Data Under General Data Protection Regulation (GDPR)

If you are from the European Economic Area (EEA), CLPS, LLC's legal basis for collecting and using the personal information described in this Privacy Policy depends on the Personal Data we collect and the specific context in which we collect it.

CLPS, LLC may collect and process your Personal Data because:

- We need to perform a contract with you
- You have given us permission to do so
- The processing or collection is in our legitimate business interests and it's not overridden by your rights
- The processing or collection is in your vital interests and is not overridden by your rights
- To comply with the law
- The school where you are enrolled has provided your Personal Data, for the purposes of your safety and protection
- Your employer has provided your Personal Data, for the purposes of your safety and protection

Retention of Data

CLPS, LLC will retain your Personal Data only for as long as is necessary for the purposes set out in this Privacy Policy. We will retain and use your Personal Data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies.

CLPS, LLC will also retain Usage Data for internal analysis purposes. Usage Data is generally retained for a shorter period of time, except when this data is used to strengthen the security or to improve the functionality of our Service, or we are legally obligated to retain this data for longer time periods.

Transfer Of Data

Your information, including Personal Data, may be transferred to and maintained on computers located outside of your state, province, country or other governmental jurisdiction where the data protection laws may differ than those from your jurisdiction.

If you are located outside United States and choose to provide information to us, please note that we transfer the data, including Personal Data, to United States and process it there.

Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

CLPS, LLC will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

Disclosure Of Data

Disclosure for Law Enforcement

Under certain circumstances, CLPS, LLC may be required to disclose your Personal Data if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

Legal Requirements

CLPS, LLC may disclose your Personal Data in the good faith belief that such action is necessary to:

- To comply with a legal obligation
- To protect and defend the rights or property of CLPS, LLC
- To prevent or investigate possible wrongdoing in connection with the Service
- To protect the personal safety of users of the Services or the public
- To protect against legal liability

Security Of Data

The security of your data is important to us, but remember that no method of transmission over the Internet, or method of electronic storage is 100% secure. While we strive to use commercially acceptable means to protect your Personal Data, we cannot guarantee its absolute security.

We have put in place technical, physical, and administrative safeguards to protect the Personal Information that we collect.

We take reasonable security measures to protect the security of your Personal Information. Despite our efforts to protect your Personal Information, there is always some risk that an unauthorized third party may find a way around our security systems or that transmissions of your information over the Internet may be intercepted.

The security of your Personal Information is important to us. When you enter Personal Information (including personal health information in various tools on our website), we encrypt the transmission of that information or use SSL connections (Secure Socket Layer) technology.

If you have any questions about the security of your personal information, you can contact us at privacy@clpsconsultants.com.

Data Protection Officer

CLPS has a "Data Protection Officer" who is responsible for matters relating to privacy and data protection. This Data Protection Officer may be reached at the following address:

CLPS, LLC
ATTN: Data Protection Officer
800 Corporate Drive
Suite 700
Fort Lauderdale, FL 33334
dataprotectionofficer@clpsconsultants.com

"Do Not Track" Signals

We do not support Do Not Track ("DNT"). Do Not Track is a preference you can set in your web browser to inform websites that you do not want to be tracked.

You can enable or disable Do Not Track by visiting the Preferences or Settings page of your web browser.

Your Data Protection Rights Under General Data Protection Regulation (GDPR)

If you are a resident of the European Economic Area (EEA), you have certain data protection rights. CLPS, LLC aims to take reasonable steps to allow you to correct, amend, delete, or limit the use of your Personal Data.

If you wish to be informed what Personal Data we hold about you and if you want it to be removed from our systems, please contact us.

In certain circumstances, you have the following data protection rights:

The right to access, update or to delete the information we have on you. Whenever made possible, you can access, update or request deletion of your Personal Data directly within your account settings section. If you are unable to perform these actions yourself, please contact us to assist you.

The right of rectification. You have the right to have your information rectified if that information is inaccurate or incomplete.

The right to object. You have the right to object to our processing of your Personal Data.

The right of restriction. You have the right to request that we restrict the processing of your personal information.

The right to data portability. You have the right to be provided with a copy of the information we have on you in a structured, machine-readable and commonly used format.

The right to withdraw consent. You also have the right to withdraw your consent at any time where CLPS, LLC relied on your consent to process your personal information.

Please note that we may ask you to verify your identity before responding to such requests.

You have the right to complain to a Data Protection Authority about our collection and use of your Personal Data. For more information, please contact your local data protection authority in the European Economic Area (EEA).

Service Providers

We may employ third party companies and individuals to facilitate our Services ("Service Providers"), to provide the Services on our behalf, to perform Service-related services or to assist us in analyzing how our Services are used.

These third parties have access to your Personal Data only to perform these tasks on our behalf and are obligated not to disclose or use it for any other purpose.

Analytics

We may use third-party Service Providers to monitor and analyze the use of our Service.

Google Analytics

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our Service. This data is shared with other Google services. Google may use the collected data to contextualize and personalize the ads of its own advertising network.

For more information on the privacy practices of Google, please visit the Google Privacy Terms web page: <http://www.google.com/intl/en/policies/privacy/>

Sentry.io

Sentry.io provides error-tracking for our Services under which it collects data to enable us to operate the Services effectively, and to provide you with the best experiences on our

website and our Services. For more information on the privacy practices of Sentry.io, please visit its privacy policy at web page: <https://sentry.io/privacy/>

Behavioral Remarketing

CLPS, LLC uses remarketing services to advertise on third party websites to you after you visited our Service. We and our third-party vendors use cookies to inform, optimize and serve ads based on your past visits to our Service.

Google AdWords

Google AdWords remarketing service is provided by Google Inc.

You can opt-out of Google Analytics for Display Advertising and customize the Google Display Network ads by visiting the Google Ads Settings page:

<http://www.google.com/settings/ads>

Google also recommends installing the Google Analytics Opt-out Browser Add-on - <https://tools.google.com/dlpage/gaoptout> - for your web browser. Google Analytics Opt-out Browser Add-on provides visitors with the ability to prevent their data from being collected and used by Google Analytics.

For more information on the privacy practices of Google, please visit the Google Privacy Terms web page: <http://www.google.com/intl/en/policies/privacy/>

Links To Other Sites

Our Services may contain links to other sites that are not operated by us. If you click on a third party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third party sites or services.

CHILDREN'S PRIVACY POLICY

We are committed to protecting the privacy of children who use our Services. This section of our Privacy Policy explains our information collection, disclosure, and parental consent practices with respect to information provided by or on behalf of children under the age of 13 ("child" or "children"), and uses terms that are defined in our general Privacy Policy. This policy is in accordance with the U.S. Children's Online Privacy Protection Act ("COPPA"), and outlines our practices in the United States regarding children's personal information.

If you have questions or concerns about our privacy practices, please contact us at privacy@clpsconsultants.com.

THE INFORMATION WE COLLECT FROM CHILDREN, HOW WE USE IT, AND HOW AND WHEN WE COMMUNICATE WITH PARENTS

We offer our Services to users of all ages and our Services are not targeted specifically to children. However, our Services are provided to protect the safety and security of students,

employees and guests of schools, government facilities, or employers, and as such we may collect information from children for that purpose. Below we summarize potential instances of collection and outline how and when we will provide parental notice and/or seek parental consent. In any instance that we collect personal information from a child, we will retain that information only so long as reasonably necessary to fulfill the activity request or allow the child to continue to participate in the activity, and ensure the security of our users and our services, or as required by law. In the event we discover we have collected information from a child in a manner inconsistent with COPPA's requirements, we will either delete the information or immediately seek the parent's consent for that collection.

Personal Data we may collect from, about or concerning children may include, but are not limited to the following:

- Email address
- First name and last name
- Phone number
- Cookies and Usage Data
- Class or school enrollment or attendance

About the collection of parent email address: Consistent with the requirements of COPPA, when so required, we will ask for a parent or guardian email address before we collect any personal information from the child. If you believe your child is participating in an activity that collects personal information and you or another parent/guardian have NOT received an email providing notice or seeking your consent, please feel free to contact us at privacy@clpsconsultants.com. We will not use parent emails provided for parental consent purposes to market to the parent, unless the parent has expressly opted in to email marketing or has separately participated in an activity that allows for such email contact.

About Verifiable Parental Consent:

Email Consent. In the event we wish to collect personal information from a child, COPPA requires that we first seek a parent or guardian's consent by email, except as explained below in the case of *school based activities*. In the email we will explain what information we are collecting, how we plan to use it, how the parent can provide consent, and how the parent can revoke consent. If we do not receive parental consent within a reasonable time, we will delete the parent contact information and any other information collected from the child in connection with that activity.

Teacher consent in lieu of a parent. With regard to *school-based activities*, COPPA allows teachers and school administrators to act in the stead of parents to provide consent for the collection of personal information from children. Schools should always notify parents about these activities. For more information on parental rights with respect to a child's educational record under the Family Educational Rights and Privacy Act (FERPA), please visit the [FERPA](#) site.

Email or Online Contact with a Child

On occasion, in order to respond to a question or request from a child, we may need to ask for the child's online contact information, such as an email address or mobile number. We will delete this information immediately after responding to the question or request.

In connection with the Services, we may collect a child's online contact information, such as an email address or mobile number, in order to communicate with the child more than once. In such instances we will retain the child's online contact information to honor the request and for no other purpose such as marketing.

Push Notifications

Push notifications are notifications on mobile and other devices that are typically associated with downloaded applications, and which can communicate to the device holder even when the application is not in use. Unless we have otherwise been given COPPA compliant consent from a teacher, school administrator or official, we will (i) require a child to provide a parent email address before the child can receive push notifications from our child-directed applications that collect a device identifier; (ii) provide the parent with notice of our contact with the child and will provide the parent the opportunity to prevent further notifications; and we will not associate the device identifier with other personal information without contacting the parent to get consent.

Geolocation Data

If our Services collects geolocation information that is specific enough to equate to the collection of a street address, we will first seek parental consent via email, unless we have otherwise been given COPPA compliant consent from a teacher or school administrator or official.

Persistent Identifiers

When children interact with us, certain information may automatically be collected, both to make our sites and applications more interesting and useful to children and for various purposes related to our business. Examples include the type of computer or mobile operating system, the child's IP address or mobile device identifier, the web browser, the frequency with which the child visits various parts of our sites or applications, and information regarding the online or mobile service provider. This information is collected using technologies such as cookies, flash cookies, web beacons, and other unique identifiers. This information may be collected by us or by a third party. This data is principally used for internal purposes only, in order to:

- provide children with access to features on our sites, applications and Services
- customize content and improve our sites and applications
- conduct research and analysis to address the performance of our sites and applications
- generate anonymous reporting for use by us

In the event we collect (or allow others to collect) such information from children on our sites and applications for other purposes, we will notify parents and obtain consent prior to such collection.

WHEN INFORMATION COLLECTED FROM CHILDREN IS AVAILABLE TO OTHERS; PARENTAL CHOICES AND CONTROLS

At any time, parents can refuse to permit us to collect further personal information from their children in association with a particular account, and can request that we delete from our records the personal information we have collected in connection with that account. Please keep in mind that a request to delete records may lead to a termination of an account, membership, or other Services.

Parents may contact us to request access to, change, or delete their child's personal information by sending an email to us at privacy@clpsconsultants.com. A valid request to delete personal information will be accommodated within a reasonable time.

Any other inquiries may be directed to:

CLPS, LLC

ATTN: Privacy Officer

800 Corporate Drive

Suite 700

Fort Lauderdale, FL 33334

Email: privacy@clpsconsultants.com

In any correspondence such as e-mail or mail, please include the child's username, the name of the school or facility to which the account corresponds, and the parent's email address and telephone number. To protect children's privacy and security, we will take reasonable steps to help verify a parent's identity before granting access to any personal information.

CHANGES TO THIS PRIVACY POLICY

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page.

We will let you know via email and/or a prominent notice on our Service, prior to the change becoming effective and update the "effective date" at the top of this Privacy Policy.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

Contact Us

If you have any questions about this Privacy Policy, please contact us:

- By email: privacy@clpsconsultants.com
- By visiting this page on our website: <http://www.clpsconsultants.com/privacy>
- By mail: CLPS, LLC
ATTN: Data Protection Officer
800 Corporate Drive
Suite 700
Fort Lauderdale, FL 33334

----- Effective January 1, 2020 -----

The foregoing section of this Privacy Policy is effective on January 1, 2020 and pertains to you if you are a resident of the State of California, or are otherwise subject to the California Consumer Privacy Act of 2018 ("CCPA")

Legal Basis for Processing Personal Data Under the CCPA

If you reside in the State of California, or are otherwise subject to the CCPA, CLPS, LLC's legal basis for collecting and using the personal information described in this Privacy Policy depends on the Personal Data we collect and the specific context in which we collect it.

CLPS, LLC may collect and process your Personal Data because:

- We need to perform a contract with you
- You have given us permission to do so
- The processing or collection is in our legitimate business interests and it's not overridden by your rights
- The processing or collection is in your vital interests and is not overridden by your rights
- To comply with the law
- The school where you are enrolled has provided your Personal Data, for the purposes of your safety and protection
- Your employer has provided your Personal Data, for the purposes of your safety and protection