Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

EDUTECH

CONTRACT ADDENDUM

Protection of Student Personally Identifiable Information

1. Applicability of This Addendum

The Wayne-Finger Lakes BOCES/EduTech) and CLPS, LLC **("Vendor")** are parties to a contract dated 12/21/2023 ("the underlying contract") governing the terms under which BOCES accesses, and Vendor provides, TAP App fourDscape ("Product"). Wayne-Finger Lakes BOCES/EduTech use of the Product results in Vendor receiving student personally identifiable information as defined in New York Education Law Section 2-d and this Addendum. The terms of this Addendum shall amend and modify the underlying contract and shall have precedence over terms set forth in the underlying contract and any online Terms of Use or Service published by Vendor.

2. Definitions

2.1. "Protected Information", as applied to student data, means "personally identifiable information" as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act (FERPA) where that information is received by Vendor from BOCES or is created by the Vendor's product or service in the course of being used by BOCES.

2.2. "Vendor" means CLPS, LLC.

2.3. "Educational Agency" means a school BOCES, board of cooperative educational services, school, or the New York State Education Department; and for purposes of this Contract specifically includes Wayne-Finger Lakes BOCES/EduTech.

2.4. "BOCES" means the Wayne-Finger Lakes BOCES/EduTech.

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

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

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

2.8. "Assignee" and "Subcontractor" shall each mean any person or entity that receives, stores, or processes Protected Information covered by this Contract from Vendor for the purpose of enabling or assisting Vendor to deliver the product or services covered by this Contract.

2.9. "This Contract" means the underlying contract as modified by this Addendum.

3. Vendor Status

Vendor acknowledges that for purposes of New York State Education Law Section 2-d it is a third-party contractor, and that for purposes of any Protected Information that constitutes education records under the Family Educational Rights and Privacy Act (FERPA) it is a school official with a legitimate educational interest in the educational records.

4. Confidentiality of Protected Information

Vendor agrees that the confidentiality of Protected Information that it receives, processes, or stores will be handled in accordance with all state and federal laws that protect the confidentiality of Protected Information, and in accordance with the BOCES Policy on Data Security and Privacy, a copy of which is Attachment B to thisAddendum.

5. Vendor Employee Training

Vendor agrees that any of its officers or employees, and any officers or employees of any Assignee of Vendor, who have access to Protected Information will receive training on the federal and state law governing confidentiality of such information prior to receiving access to that information.

6. No Use of Protected Information for Commercial or Marketing Purposes

Vendor warrants that Protected Information received by Vendor from BOCES or by any Assignee of Vendor, shall not be sold or used for any commercial or marketing purposes; shall not be used by Vendor or its Assignees for purposes of receiving remuneration, directly or indirectly; shall not be used by Vendor or its Assignees for advertising purposes; shall not be used by Vendor or its Assignees to develop or improve a product or service; and shall not be used by Vendor or its Assignees to market products or services to students.

7. Ownership and Location of Protected Information

7.1. Ownership of all Protected Information that is disclosed to or held by Vendor shall remain with BOCES. Vendor shall acquire no ownership interest in education records or Protected Information.

7.2. BOCES shall have access to the BOCES's Protected Information at all times through the term of this Contract. BOCES shall have the right to import or export Protected Information in piecemeal or in its entirety at their discretion, without interference from Vendor.

7.3. Vendor is prohibited from data mining, cross tabulating, and monitoring data usage and access by BOCES or its authorized users, or performing any other data analytics other than those required to provide the Product to BOCES. Vendor is allowed to perform industry standard back-ups of Protected Information. Documentation of back-up must be provided to BOCES upon request.

7.4. All Protected Information shall remain in the continental United States (CONUS) or Canada. Any Protected Information stored, or acted upon, must be located solely in data centers in CONUS or Canada. Services which directly or indirectly access Protected Information may only be performed from locations within CONUS or Canada. All helpdesk, online, and support services which access any Protected Information must be performed from within CONUS or Canada.

8. Purpose for Sharing Protected Information

The exclusive purpose for which Vendor is being provided access to Protected Information is to provide the product or services that are the subject of this Contract to Wayne-Finger Lakes BOCES/EduTech.

9. Downstream Protections

Vendor agrees that, in the event that Vendor subcontracts with or otherwise engages another entity in order to fulfill its obligations under this Contract, including the purchase, lease, or sharing of server space owned by another entity, that entity shall be deemed to be an "Assignee" of Vendor for purposes of Education Law Section 2-d, and Vendor will only share Protected Information with such entities if those entities are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of Vendor under this Contract and all applicable New York State and federal laws.

10. Protected Information and Contract Termination

10.1. The expiration date of this Contract is defined by the underlying contract.

10.2. Upon expiration of this Contract without a successor agreement in place, Vendor shall assist BOCES in exporting all Protected Information previously received from, or then owned by, BOCES.

10.3. Vendor shall thereafter securely delete and overwrite any and all Protected Information 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 of shared data) as well as any and all Protected Information maintained on behalf of Vendor in secure data center facilities.

10.4. Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

10.5. 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 removed) derived from Protected Information, they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10.6. Upon request, Vendor and/or its subcontractors or assignees will provide a certification to BOCES from an appropriate officer that the requirements of this paragraph have been satisfied in full.

11. Data Subject Request to Amend Protected Information

11.1. In the event that a parent, student, or eligible student wishes to challenge the accuracy of Protected Information that qualifies as student data for purposes of Education Law Section 2-d, that challenge shall be processed through the procedures provided by the BOCES for amendment of education records under the Family Educational Rights and Privacy Act (FERPA).

11.2. Vendor will cooperate with BOCES in retrieving and revising Protected Information, but shall not be responsible for responding directly to the data subject.

12. Vendor Data Security and Privacy Plan

12.1. Vendor agrees that for the life of this Contract the Vendor will maintain the administrative, technical, and physical safeguards described in the Data Security and Privacy Plan set forth in Attachment C to this Contract and made a part of this Contract.

12.2. Vendor warrants that the conditions, measures, and practices described in the Vendor's Data Security and Privacy Plan:

12.3. align with the NIST Cybersecurity Framework 1.0;

12.4. equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection;

12.5. outline how the Vendor will implement all state, federal, and local data security and privacy contract requirements over the life of the contract, consistent with the BOCES data security and privacy policy (Attachment B);

12.6. specify the administrative, operational and technical safeguards and practices it has in place to protect Protected Information that it will receive under this Contract;

12.7. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;

12.8. specify how officers or employees of the Vendor and its assignees who have access to Protected Information receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

12.9. specify if the Vendor will utilize sub-contractors and how it will manage those relationships and contracts to ensure Protected Information is protected;

12.10. specify how the Vendor will manage data security and privacy incidents that implicate Protected Information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify BOCES; and

12.11. describe whether, how and when data will be returned to BOCES, transitioned to a successor contractor, at BOCES's option and direction, deleted or destroyed by the Vendor when the contract is terminated orexpires.

13. Additional VendorResponsibilities

Vendor acknowledges that under Education Law Section 2-d and related regulations it has the following obligations with respect to any Protected Information, and any failure to fulfill one of these statutory obligations shall be a breach of this Contract:

13.1 Vendor shall limit internal access to Protected Information to those individuals and Assignees or subcontractors that need access to provide the contracted services;

13.2 Vendor will not use Protected Information for any purpose other than those explicitly authorized in this Contract;

13.3 Vendor will not disclose any Protected Information to any party who is not an authorized representative of the Vendor using the information to carry out Vendor's obligations under this Contract or to the BOCES unless (1) Vendor has the prior written consent of the parent or eligible student to disclose the information to that party, or (ii) the disclosure is required by statute or court order, and notice of the disclosure is provided to BOCES no later than the time of disclosure, unless such notice is expressly prohibited by the statute or court order;

13.4 Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of Protected Information in its custody;

13.5 Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2);

13.6 Vendor will notify the BOCES of any breach of security resulting in an unauthorized release of student data by the 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 but no more than seven calendar days after the discovery of the breach; and

Where a breach or unauthorized disclosure of Protected Information is attributed to the Vendor, the Vendor shall pay for or promptly reimburse BOCES for the full cost incurred by BOCES to send notifications required by Education Law Section 2-d.

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Signatures

For Wayne-Finger Lakes BOCES/EduTech

Date 1/2/24

mel

Date CPS, LLC

12/21/2023

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment A – Parent Bill of Rights for Data Security and Privacy

Wayne-Finger Lakes BOCES (EduTech)

Parents' Bill of Rights for Data Privacy and Security

The Wayne-Finger Lakes BOCES (EduTech)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 BOCES and school operations.

The Wayne-Finger Lakes BOCES (EduTech)seeks to insure 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 Wayne-Finger Lakes BOCES (EduTech) 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 Board Policy 5500 entitled Family Educational Rights and Privacy Act(FERPA).
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 http://www.nysed.gov/data-privacy-security/student-data-inventory 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 the Chief Privacy Officer, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

Revised October 2019

Signatures

For Wayne-Finger Lakes BOCES/EduTech	**For (Vendor Name)**
	CLPS, LLC
Date	**Date**
1/2/24	12/21/2023

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment B – Wayne-Finger Lakes BOCES/EduTech Data Privacy and Security Policy

In accordance with New York State Education Law §2-d, the BOCES hereby implements the requirements of Commissioner's regulations (8 NYCRR §121) and aligns its data security and privacy protocols with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (NIST Cybersecurity Framework or "NIST CSF").

In this regard, every use and disclosure of personally identifiable information (PII) by the BOCES will benefit students and the BOCES (for example, improving academic achievement, empowering parents and students with information, and/or advancing efficient and effective school operations). PII will not be included in public reports or other documents.

The BOCES also complies with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Consistent with FERPA's requirements, unless otherwise permitted by law or regulation, the BOCES will not release PII contained in student education records unless it has received a written consent (signed and dated) from a parent or eligible student. For more details, see Policy 6320 and any applicable administrative regulations.

In addition to the requirements of FERPA, the Individuals with Disabilities Education Act (IDEA) provides additional privacy protections for students who are receiving special education and related services. For example, pursuant to these rules, the BOCES will inform parents of children with disabilities when information is no longer needed and, except for certain permanent record information, that such information will be destroyed at the request of the parents. The BOCES will comply with all such privacy provisions to protect the confidentiality of PII at collection, storage, disclosure, and destruction stages as set forth in federal regulations 34 CFR 300.610 through 300.627.

The Board of Education values the protection of private information of individuals in accordance with applicable law and regulations. Further, the BOCES Director of Educational Technology is required to notify parents, eligible students, teachers and principals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy and New York State Education Law §2-d

a) "Private information" shall mean **personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

1. Social security number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password, which would permit access to an individual's financial account.
4. Any additional data as it relates to administrator or teacher evaluation (APPR)

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

**"Personal information" shall mean any information concerning a person, which, because of name, number, symbol, mark or other identifier, can be used to identify that person.

b) Personally Identifiable Information, as applied to student data, means 40 personally identifiable information as defined in section 99.3 of Title 34 of the Code of 41 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 42 U.S.C 1232-g, and as applied to teacher and principal data, means personally 43 identifying information as such term is defined in Education Law §3012-c(10).

c) Breach means the unauthorized access, use, or disclosure of student data 9 and/or teacher or principal data. Good faith acquisition of personal information by an employee or agent of the BOCES for the purposes of the BOCES is not a breach of the security of the system, provided that private information is not used or subject to unauthorized disclosure.

Notification Requirements
Methods of Notification

The required notice shall be directly provided to the affected persons and/or their guardians by one of the following methods:

a) Written notice;

b) Secure electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and a log of each such notification is kept by the BOCES when notifying affected persons in electronic form. However, in no case shall the BOCES require a person to consent to accepting such notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

Regardless of the method by which notice is provided, the notice shall include contact information for the notifying BOCES and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired. This notice shall take place 60 days of the initial discovery.

In the event that any residents are to be notified, the BOCES shall notify the New York State Chief Privacy Officer, the New York State Cyber Incident Response Team, the office of Homeland Security, and New York State Chief Security Officer as to the timing, content and distribution of the notices and approximate number of affected persons. Such notice shall be made without delaying notice to affected residents.
The Superintendent or his/her designee will establish and communicate procedures for parents, eligible students, and employees to file complaints about breaches or unauthorized releases of student, teacher or principal data (as set forth in 8 NYCRR §121.4). The Superintendent is also authorized to promulgate any and all other regulations necessary and proper to implement this policy.

Data Protection Officer

The BOCES has designated a BOCES employee to serve as the BOCES's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the BOCES.

The BOCES will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1 (1988; rev. 2004).

Annual Data Privacy and Security Training

The BOCES will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations.

References:

Education Law §2-d

8 NYCRR §121

Family Educational Rights and Privacy Act of 1974, 20 USC §1232(g), 34 CFR 99

Individuals with Disabilities Education Act (IDEA), 20 USC §1400 et seq., 34 CFR 300.610–300.627

Educational
Technology Service
Genesee Valley
Wayne-Finger Lakes

Attachment C – Vendor's Data Security and Privacy Plan

The Wayne-Finger Lakes BOCES Parents Bill of Rights for Data Privacy and Security, which is included as Attachment B to this Addendum, is incorporated into and make a part of this Data Security and Privacy Plan.

(Vendor can attach)

Addendum B

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM

1. **EXCLUSIVE PURPOSES FOR DATA USE**: The exclusive purposes for which "student data" or "teacher or principal data" (as those terms are defined in Education Law Section 2-d and collectively referred to as the "Confidential Data") will be used by CLPS, LLC (the "Contractor") are limited to the purposes authorized in the contract between the Contractor and the Wayne-Finger Lakes BOCES/EduTech (the "BOCES") dated 12/21/2023 (the "Contract").

2. **SUBCONTRACTOR OVERSIGHT DETAILS**: The Contractor will ensure that any subcontractors, or other authorized persons or entities to whom the Contractor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., the Family Educational Rights and Privacy Act ("FERPA"); Education Law §2-d; 8 NYCRR Part 121).

3. **CONTRACT PRACTICES**: The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the BOCES in **CSV (insert data format)** format and/or destroyed by the Contractor as directed by the BOCES.

4. **DATA ACCURACY/CORRECTION PRACTICES**: A parent or eligible student can challenge the accuracy of any "education record", as that term is defined in FERPA, stored by the BOCES in a Contractor's product and/or service by following the BOCES' procedure for requesting the amendment of education records under FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by the BOCES in Contractor's product and/or service by following the appeal procedure in the BOCES' APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

5. **SECURITY PRACTICES**: Confidential Data provided to Contractor by the BOCES will be stored AWSRDS (**insert location**). The measures that Contractor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.

6. **ENCRYPTION PRACTICES**: The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Signature:

Date:12/21/2023

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