

ATTACHMENT A
AGREEMENT BETWEEN
THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA
AND
PUBLIC CONSULTING GROUP, LLC
STANDARD STUDENT DATA PRIVACY AGREEMENT

This Student Data Privacy Agreement (“**DPA**”), as developed by the Student Data Privacy Consortium (“**SDPC**”) and as modified by The School Board of Citrus County, Florida is entered into on the date of full execution (the “**Effective Date**”) and is entered into by and between:

The School Board of Citrus County, Florida, located at 1007 W. Main Street, Inverness, Florida 34450 (the “**LEA**”)

and

Public Consulting Group LLC, located at 148 State Street, Boston, Massachusetts 02109 (the “**Provider**”).

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

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

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

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

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

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

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

✓ If checked, LEA and Provider agree to the additional terms or modifications set forth in **Exhibit "H"**. (Optional)

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

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

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

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

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

The designated representative for the LEA for this DPA is:

Name: Jennifer Greco

Title: Coordinator, District Student Services

Address: 1007 W. Main Street, Inverness, Florida 34450

Phone: 352-527-0090


Email: grecoj@citruschools.org

The designated representative for the Provider for this DPA is:


Name: Daniel Wistman
Title: Manager
Address: 148 State Street, Boston, MA 02109
Phone: (617) 817-2855
Email: dwistman@pcgus.com

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

LEA: The School Board of Citrus County, Florida.

Signature:  _____
Printed Name: Douglas A. Dodd
Title: Chairman
Date: 8/8/23

Provider: Public Consulting Group, LLC

Signature:  _____
Printed Name: Daniel Wistman
Title: Manager
Date: 9/1/2023

STANDARD CLAUSES

Version 1.0

Article I. ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data
2. **Student Data to Be Provided.** In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
3. **DPA Definitions.** The definition of terms used in this DPA is found in **Exhibit “C”**. In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

Article II. ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA.** All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty-five (45) days from the date

of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account.** If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.
4. **Law Enforcement Requests.** Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.
5. **Subprocessors.** Provider shall enter into written Agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

Article III. ARTICLE III: DUTIES OF LEA

1. **Provide Data in Compliance with Applicable Laws.** LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.
2. **Annual Notification of Rights.** If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

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

Article IV. ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.
2. **Authorized Use.** The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in **Exhibit "A"** or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.
3. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality Agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.
4. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other non- public information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.
 - (a) **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Student Data. De- Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written

notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA's written approval of the manner in which De-Identified Data is presented.

5. **Disposition of Data**. Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a **"Directive for Disposition of Data"** form, a copy of which is attached hereto as **Exhibit "D"**. If the LEA and Provider employ **Exhibit "D"**, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in **Exhibit "D"**.
6. **Advertising Limitations**. Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits.

Article V. ARTICLE V: DATA PROVISIONS

1. **Data Storage**. Where required by applicable law, Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored.
2. **Audits**. No more than once a year, or following unauthorized access, upon receipt of a written request from the LEA with at least ten (10) business days' notice and upon the execution of an appropriate confidentiality Agreement, the Provider will allow the LEA to audit the security and privacy measures that are in place to ensure protection of Student Data or any portion thereof as it pertains to the delivery of services to the LEA. The Provider will cooperate reasonably with the LEA and any local, state, or federal agency with oversight authority or jurisdiction in connection with any audit or investigation of the Provider and/or

delivery of Services to students and/or LEA, and shall provide reasonable access to the Provider's facilities, staff, agents and LEA's Student Data and all records pertaining to the Provider, LEA and delivery of Services to the LEA. Failure to reasonably cooperate shall be deemed a material breach of the DPA.

3. **Data Security.** The Provider agrees to utilize administrative, physical, and technical safeguards designed to protect Student Data from unauthorized access, disclosure, acquisition, destruction, use, or modification. The Provider shall adhere to any applicable law relating to data security. The provider shall implement an adequate Cybersecurity Framework based on one of the nationally recognized standards set forth in **Exhibit "F"**. Exclusions, variations, or exemptions to the identified Cybersecurity Framework must be detailed in an attachment to **Exhibit "H"**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit "F"**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who LEA may contact if there are any data security concerns or questions.
4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within seventy-two (72) hours of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident. Provider shall follow the following process:
 - (1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
 - i. The name and contact information of the reporting LEA subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - iv. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.
- (3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.
- (4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.
- (5) In the event of a breach originating from LEA's use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

Article VI. ARTICLE VI: GENERAL OFFER OF TERMS

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

Article VII. MISCELLANEOUS

1. **Termination.** In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service Agreement or contract if the other party breaches any terms of this DPA.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of LEA's Student Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license Agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between **Exhibit "H"**, the SDPC Standard Clauses, and/or the

Supplemental State Terms, **Exhibit "H"** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. **Entire Agreement.** This DPA and the Service Agreement constitute the entire Agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or Agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.
5. **Severability.** Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.
6. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.
7. **Successors Bound:** This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business. In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the

DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. **Authority**. Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or Contractors who may have access to the Student Data and/or any portion thereof.
9. **Waiver**. No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both Parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

EXHIBIT "A"

DESCRIPTION OF SERVICES

The PCG Behavioral Threat Assessment Management (BTAM) solution is built the EDPlan case management platform which provides many behavioral related pathways. The EDPlan platform is designed with a student-centered focus using a whole child case management approach in order that interventions can be prescribed, delivered and monitored for effectiveness. The BTAM solution fully supports school based teams in evaluating threats to others and threats to self while providing full HIPAA and FERPA compliance. The solution allows automated notification of existing threats within the school district and includes threats to others and threats to self. The evidenced-based solution assists in the consistent, structured approach for multidisciplinary teams to identify and support students who present a potential risk of violence/aggression, self-harm, or other concerning behaviors. Our solution helps school personnel identify students who are exhibiting behaviors along the pathway to violence and intervene with supports designed to de-escalate those behaviors in order to mitigate risk.

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	X
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications captured (emails, blog entries)	X
Conduct	Conduct or behavioral data	X
Demographics	Date of Birth	X
	Place of Birth	
	Gender	X
	Ethnicity or race	X
	Language information (native, or primary language spoken by student)	X

Category of Data	Elements	Check if Used by Your System
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	X
	Student grade level	X
	Homeroom	X
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	
Schedule	Student scheduled courses	X
	Teacher names	X
Special Indicator	English language learner information	X
	Low income status	X
	Medical alerts/ health data	X

Category of Data	Elements	Check if Used by Your System
	Student disability information	X
	Specialized education services (IEP or 504)	X
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	X
	State ID number	X
	Provider/App assigned student ID number	X
	Student app username	
	Student app passwords	
Student Name	First and/or Last	X
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	X
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	X

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

EXHIBIT “C”

DEFINITIONS

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

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

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

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

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

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

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

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

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

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

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

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

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such

student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

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

EXHIBIT "D"

DIRECTIVE FOR DISPOSITION OF DATA

[Insert Name of District or LEA] Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

X ____ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

____ Disposition shall be by destruction or deletion of data.

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

Data transfer will occur to the Technology Resource Center.
Specific instructions will be given with the termination of services documentation at that time.

3. Schedule of Disposition

Data shall be disposed of by the following date:

____ As soon as commercially practicable.

____ By **[Insert Date]**

4. Signature



Authorized Representative of LEA

8/8/23

Date

5. Verification of Disposition of Data



Authorized Representative of Provider

9/1/2023

Date

1. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Provider, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and the Provider shall therefore be bound by the same terms of this DPA for the term of the DPA between the **[Insert Name of Originating LEA]** and the Provider. ****PRIOR TO ITS EFFECTIVENESS, SUBSCRIBING LEA MUST DELIVER NOTICE OF ACCEPTANCE TO PROVIDER PURSUANT TO ARTICLE VII, SECTION 5. ****

The School Board of Citrus County, Florida

BY: 

Date: 8/8/23

Printed Name: Douglas A. Dodd

Title/Position: Chairman

SCHOOL DISTRICT NAME: THE SCHOOL BOARD OF CITRUS COUNTY, FLORIDA
DESIGNATED REPRESENTATIVE OF LEA:

Name; **Douglas A. Dodd**

Title: School Board Chairman

Address: 1007 W. Main Street, Inverness. FL 34450

Telephone Number: 352-726-1931

Email: doddd@citruschools.org

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity

Frameworks 2/24/2020

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

Cybersecurity Frameworks

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

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

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

EXHIBIT “G”

Supplemental SDPC State Terms for [State]

Version _____

[The State Supplement is an ***optional*** set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual Parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit “H”** in this proposed structure).]

EXHIBIT "H"

Additional Terms or Modifications

THIS EXHIBIT "H" effective simultaneously with attached Student Data Privacy Agreement ("DPA") between The School Board of Citrus County, Florida, (the "Local Education Agency" or "LEA") and Public Consulting Group, LLC (the "Provider") is incorporated in the attached DPA and amends the DPA (and all supplemental terms and conditions and policies applicable to the DPA) as follows:

1. The second WHEREAS CLAUSE is amended to add "the Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98)" after "15 U.S.C. § 6501-6506 (16 CFR Part 312)".
2. Paragraph 3 on the page 2 of the DPA is deleted in its entirety and replaced with the following: In the event of a conflict between the DPA Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including Provider Terms of Service or Privacy Policy, the terms of Technology Master Service Agreement, and then this DPA shall control.
3. The last sentence of Article II, Paragraph 1 is amended as follows: Provider agrees that for purposes of this Agreement, it will be designated a "School Official," under the control and direction of the LEA as it pertains to the use of Student Data, with "legitimate educational interests" as those terms have been interpreted and defined under FERPA. Provider may transfer student-generated content to a separate account, according to the procedures set forth below. Provider agrees to abide by FERPA and Fla. Stat. 1002.22 while performing its service for the LEA.
4. Article I, Paragraph 2 is amended to add the following: Indemnification. Provider shall indemnify, hold harmless, and defend the SB and all of SB's current, past, and future officers, agents, and employees (collectively, "Indemnified Party") from and against any and all causes of action, demands, claims, losses, liabilities, and expenditures of any kind, including attorneys' fees, court costs, and expenses, including through the conclusion of any appellate proceedings, raised or asserted by any person or entity not a party to this Agreement, and caused or alleged to be caused, in whole or in part, by any breach of this Agreement by Provider, third-Parties, or subprocessor(s) related to Attachment A, Exhibit B (Schedule of Data), including but not limited to, failure to notify the SB of any additional students' PII collected and not updated by Provider in Exhibit B.

5. Article II, Paragraph 5 is deleted in its entirety and replaced with the following: Provider shall enter into written Agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner consistent with the terms of this DPA. Provider agrees to share the Subprocessors names and Agreements with LEA upon LEA's request.
6. Article III, Paragraph 1 is amended to add the following sentence: LEA will allow Provider access to Student Data necessary to perform the Services and pursuant to the terms of this DPA and in compliance with FERPA, COPPA, PPRA, and all other privacy statutes cited in this DPA.
7. Article IV, Paragraph 1 is amended to add the following sentence: The Parties expect and anticipate that Provider may receive personally identifiable information in education records from the District only as an incident of service or training that Provider provides to the LEA pursuant to this Agreement. The Provider shall comply with all applicable State and Federal laws and regulations pertaining to Student Data privacy and security, including FERPA, COPPA, PPRA, Florida Statutes Sections 1001.41 and 1002.22, and all other privacy statutes cited in this DPA. The Parties agree that Provider is a "school official" under FERPA and has a legitimate educational interest in personally identifiable information from education records because for purposes of the contract, Provider: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records
8. Article IV, Paragraph 2 is amended to add the following sentence: Provider also acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, meta Student Data, user content or other non-public information and/or personally identifiable information contained in the Student Data, without the express written consent of the LEA.
9. Article IV, Paragraph 7 is deleted in its entirety and replaced with the following: Provider is prohibited from using or selling Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, targeted advertising, or other commercial efforts by Provider; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Student Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This

section does not prohibit Provider from generating legitimate personalized learning recommendations.

10. Article V, Paragraph 1 is deleted in its entirety and replaced with the following: Student Data shall be stored within the United States. Upon request of the LEA, Provider will provide a list of the locations where Student Data is stored. Provider shall not, without the express prior written consent of District: Transmit Student Data or PII to any Providers or Subprocessors located outside of the United States; distribute, repurpose or share Student Data or PII with any Partner Systems not used for providing services to the LEA; use PII or any portion thereof to inform, influence or guide marketing or advertising efforts, or to develop a profile of a student or group of students for any commercial purpose [or for any other purposes]; use PII or any portion thereof to develop commercial products or services; use any PII for any other purpose other than in connection with the services provided to the LEA; and engage in targeted advertising, based on the Student Data collected from the LEA.
11. Article V, Paragraph 4 is hereby amended to change the notification date: **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Student Data that compromises the security, confidentiality or integrity of the Student Data maintained by the Provider the Provider shall provide notification to LEA within three (3) business of confirmation of the incident, unless notification within this time limit would disrupt investigation of the incident by law enforcement. In such an event, notification shall be made within a reasonable time after the incident.
12. Article VII is hereby amended to add Paragraph 10 as follows: **Assignment.** None of the Parties to this DPA may assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of the other party to this DPA.
13. Article VII, is hereby amended to add Paragraph 11 as follows: **Click through.** Any “click through” terms and conditions or terms of use are superseded by the Technology Master Service Agreement and this DPA, and acceptance of the terms and conditions or terms of use through the “click through” do not indicate acceptance by the entity.
14. Article VII, is hereby amended to add Paragraph 12 as follows: **Security Controls.** Security Controls. Provider represents and warrants that any software licensed hereunder shall not contain any virus, worm, Trojan Horse, tracking software or be capable of identifying non-approved users or tracking any approved user, or any undocumented software locks or drop dead devices that would render inaccessible or impair in any way the operation of the software or any other hardware, software or

data for which the software is designed to work with.

15. Article VII, is hereby amended to add Paragraph 13 as follows: **Authority to Execute Agreement.** Each person signing this Agreement on behalf of either Party individually warrants that he or she has full legal power to execute this Agreement on behalf of the Party for whom he or she is signing, and to bind and obligate such Party with respect to all provisions contained in this Agreement.

THE PARTIES REPRESENT THAT THEY HAVE THOROUGHLY DISCUSSED ALL ASPECTS OF THE AGREEMENT AND ADDENDUM WITH THEIR RESPECTIVE ATTORNEY(S), THAT THEY FULLY UNDERSTAND ALL OF ITS PROVISIONS, AND THAT THEY ARE VOLUNTARILY ENTERING INTO THE AGREEMENT AND ADDENDUM WITH THE FULL KNOWLEDGE OF ITS LEGAL SIGNIFICANCE AND WITH THE INTENT TO BE LEGALLY BOUND BY ITS TERMS.

Local Education Agency:

[Redacted]

Douglas A Dodd, Chairman

Date: 8/8/23

Provider:

[Redacted]

By: Daniel Wistman

Title: Manager

Date: 9/1/2023

ATTACHMENT B

STATEMENT OF WORK

PCG is pleased to submit the following pricing proposal¹ for the EDPlan Behavioral Threat Assessment and Suicide Risk Assessment solution.

Licensing, Support, and Maintenance Subscription (Annual cost)	
Threat Assessment Value Package	\$18,255
Behavioral Threat Assessment Subscription (60 cents per student)	(\$1.18 per student based
Self-Harm Risk Assessment Subscription (40 cents per student)	on 15,470
Subscription Includes:	student count)
<ul style="list-style-type: none"> • Live Help Desk support² • System hosting, maintenance, and <u>four</u> new releases per year • Dashboards 	
Standard package add-ons include: (18 cents per student)	
<ul style="list-style-type: none"> • Documentation of Students of Concern • Two additional risk assessment pathways: sexual misconduct and fire misuse • Florida State reporting • Advanced Reporting provided through SAP business objects • Unlimited PaperClip Document Repository for case artifacts 	
EDPlan BTA Annual Refresher Training	Included
Includes one (1) 2-hour virtual refresher training session per year	
EDPlan Notifier – Emails	Included
Includes email alerts to key parties on significant events (note: text alerts are an available option for an additional fee) ³	
Total Ongoing Annual Licensing, Support, and Maintenance	\$18,255.00

PCG BTA PROPOSAL ASSUMPTIONS:

1. Proposed pricing will be honored for 45 calendar days and assumes a three-year contract commitment.
2. After implementation, PCG shall make available qualified personnel to provide technical support, providing direction and general support on system features and functions to designated school-based trainers. We refer to this as Tier-2 support. This general technical support is included in the licensing fee and can be accessed via email or the Message Board feature of the EDPlan web-based application and does not include the provision of guidance or recommendations related to school policy, operations, instruction, or data analysis. Non-school-based training users of the system requesting support will be directed to refer to their school-based trainer for support.
3. Note text notifications are available for a fee based on volume of texts.

ATTACHMENT C

ADDITIONAL EDPLAN™ LICENSE AND RELATED SERVICES TERMS AND CONDITIONS

1. DEFINITIONS

In addition to the terms defined elsewhere in this Agreement, terms appearing in initial capital letters shall have the following meanings:

1.1. “Documentation” means all technical information, training materials, instructions, manuals, and diagrams (in printed, electronic, or other media) pertaining to the EDPlan Service.

1.2. “EDPlan Service” means: (i) the Internet-based functionality and EDPlan modules identified in this Agreement; (ii) all products and services related to such services within this scope of work; (iii) all PCG initiated Releases, Updates, and Upgrades applicable to the foregoing and offered to School District by PCG; and (iv) the Documentation developed by PCG for distribution and use in combination with the foregoing.

1.3. “Intellectual Property Rights” means patent rights, copyrights, trade secret rights, trademark rights, and any other intellectual property rights recognized by the law of each applicable jurisdiction in which PCG may market or license the EDPlan Service.

1.4. “New Releases” means any new revision of EDPlan Service that includes significant enhancements which add new features to the EDPlan Service and which generally will be designated by a new version number either to the left of the decimal point (e.g., from v2.03 to v3.00) or one decimal place to the right of the decimal point (e.g., from v2.03 to v2.10).

1.5. “Permitted Use” means use of the EDPlan Service by employees, contractors, and others affiliated with or authorized by School District only for School District’s internal education-related purposes.

1.6. “School District User” means any employee, contractor, and other authorized user of the “School District” who will be granted access to the EDPlan Service.

1.7. “Trademarks” means all trademarks, trade names, service marks, and logos now owned or hereinafter acquired by either party, and all other trademarks, trade names, service marks, and logos identifying or used in connection with their product or service offerings, whether or not registered under the laws of a particular jurisdiction or territory.

1.8. “Updates” means any new revisions and/or modifications made to the EDPlan Service and/or Documentation in order to correct operational errors.

1.9. “Upgrades” means any new revision of the EDPlan Service that includes corrections and minor modifications to existing features and which generally will be designated by a new version number which has changed from the prior number only two places to the right of the decimal point (e.g., from v2.02 to v2.03).

2. EDPLAN™ SERVICE. Subject to the terms and conditions of this Agreement, including School District's performance of its obligations hereunder, PCG shall provide the EDPlan Service (including application and related supporting services) to School District, as more fully described in the Agreement.

2.1. Grant of License for EDPlan Service. PCG grants to School District, and School District accepts, a non-exclusive, non-transferable, non-sublicensable right and license, during the Term only, to access via the Internet and use the EDPlan Service to the extent reasonably necessary in performing related school business functions.

2.2. Grant of License for Documentation. PCG grants to School District, and School District accepts, a non-exclusive, non-transferable, non-sublicensable royalty-free license under PCG's copyrights in PCG's Documentation, during the Term only:

2.2.1. to incorporate PCG's Documentation, in whole or in part, into other written materials prepared by or for School District with respect to the EDPlan Service; and

2.2.2. to reproduce and distribute modified and original versions of PCG's Documentation, in hard copy or in an on-line format, as part of School District's Documentation for the EDPlan Service, and, if such School District's Documentation is in an on-line format, allow School District Users to make print copies of the same.

2.3. Restrictions on License Grant

2.3.1. School District shall not use or grant to any person or entity other than authorized School District Users the right to use the EDPlan Service, which users shall be subject to the terms set forth herein. School District shall not distribute, market, or sublicense the EDPlan Service, and shall not permit any School District User or third party to do so.

2.3.2. School District shall not remove, modify, or suppress any confidentiality legends or proprietary notices placed on or contained within the EDPlan Service, and shall not permit any School District User or third party to do so.

2.3.3. School District shall not distribute any PCG documentation or intellectual property made available through this contract to any individual or organization that is not part of School District or an authorized School District User, and shall not permit any School District User or third party to do so.

2.3.4. School District shall not transfer, rent, or permit access to the EDPlan Service to any third party, and shall not permit any School District User or third party to do so.

2.3.5. School District shall not modify, decompile, disassemble, or otherwise attempt to reverse engineer the EDPlan Service or any portion thereof, and shall not permit any School District User or third party to do so.

2.3.6. School District shall not circumvent any security protection within the EDPlan Service and shall not permit any School District User or third party to do so.

2.4. Reservation of Rights.

2.4.1. Subject to the license rights granted to School District by this Section, all right, title, and interest in and to the EDPlan Service, including the Intellectual Property Rights and technology inherent in EDPlan Service, are and at all times will remain the sole and exclusive property of PCG. No right to use, print, copy, distribute, integrate, or display the EDPlan Service, in whole or in part, is granted in this Agreement, except as is explicitly provided in this Agreement. Nothing contained in this Agreement will directly or indirectly be construed to assign or grant to School District any right, title, or interest in or to PCG's Intellectual Property Rights or other rights in and to the EDPlan Service or PCG's Trademarks.

2.4.2. Except as expressly authorized by this Agreement, School District shall not use, display, copy, distribute, modify, or sublicense the EDPlan Service. PCG reserves all rights not expressly granted to School District by this Agreement.

3. PROPRIETARY RIGHTS; PROTECTION OF CONFIDENTIAL INFORMATION

3.1. Ownership. School District acknowledges that PCG owns the EDPlan Service, that the EDPlan Service is not generally published, and that the EDPlan Service embodies the Confidential Information of PCG. All right, title, and interest in and to the EDPlan Service, including, without limitation, all copyrights, trade secret rights, and other intellectual property rights pertaining in and to the EDPlan Service shall remain vested in PCG and its third-party licensors. PCG acknowledges that School District owns all of the data inputted by each School District User for purposes of creating an Individualized Education Plan and any and all reports produced as a result of using the EDPlan Service during the contract term.

3.2. School District Duties. School District will take reasonable steps to protect the EDPlan Service from unauthorized access, copying, dissemination, and disclosure, and from other unauthorized use, and will report promptly to PCG any such use of which School District becomes aware. School District shall be responsible for the quality, integrity, and accuracy of all data entered and used in connection with the EDPlan Service, including all deletions of such data by School District Users. School District is responsible for establishing and enforcing any School District policies related to data security, information management, account management of School District users, and the proper handling of data extracted, reported, or otherwise removed by the system by School District personnel.

3.3. PCG Duties. PCG will take reasonable steps to protect the data that School District enters as part of its use of the EDPlan Service. PCG will use technical, administrative, and physical safeguards to protect against unintentional loss and against unauthorized access, destruction, misuse, modification, and disclosure. Although no computer system or information can ever be fully protected against every possible hazard, PCG is committed to providing reasonable and appropriate security controls to protect information against foreseeable hazards. PCG recognizes that School District data is the property of School District. Upon contract termination, or at School District's request, PCG will provide all data to School District, including all database tables and a description of the table structure. PCG may keep a backup copy of the data unless otherwise agreed by the parties, subject to applicable law.

3.4. Third Party Infringement. PCG reserves the sole and exclusive right at its discretion to assert claims against third parties for infringement or misappropriation of its Intellectual Property Rights in the EDPlan Service.

4. PRODUCT MARKING. School District acknowledges that PCG is and shall remain the owner of all right, title, and interest in and to each of PCG's Trademarks in any form or embodiment thereof, and is also the owner of all goodwill associated with PCG's Trademarks. All goodwill generated by School District use of the EDPlan Service with respect to PCG's Trademarks shall inure exclusively to the benefit of PCG. School District shall promptly notify PCG of any third-party infringements of any of the PCG Trademarks used in connection with the EDPlan Service, or any act of unfair competition by third parties relating to the PCG Trademarks, within a reasonable time of School District's knowledge of such infringements or acts.

5. LIMITED WARRANTY. PCG represents and warrants that it has the right to license the EDPlan Service as specified by this Agreement, and that the use of the EDPlan Service contemplated in this Agreement does not infringe upon, violate, or constitute a misappropriation of any copyright, trademark, trade secret, or any other proprietary right of any third party. Under no circumstances will PCG be responsible for School District's hardware, software, browsers, or Internet connections that provide access to the EDPlan Service. PCG shall use reasonable efforts to maintain the EDPlan Service and to correct any problems that may arise with the use of the EDPlan Service. PCG's scheduled maintenance of the EDPlan Service, or the scheduled maintenance of PCG's Internet provider, shall not be deemed a failure to provide the EDPlan Service.

6. DISCLAIMER. Note that PCG's Threat Assessment solution is a set of tools to be used by School District's school-based inter-disciplinary threat assessment team to (1) conduct evaluations about student risk to themselves and others, and (2) allow such teams to then determine independently any follow-up steps to monitor and support students. The Threat Assessment solution does not render any determinations or conclusions. It uses nationally recognized guidelines and frameworks that provides School District's inter-disciplinary teams the ability to document threats and incidents, evaluate students, and render the team's its own assessments, conclusions, and support decisions. The Threat Assessment solution should not be construed as determining actions or decisions upon which School District must or should rely.

