

This Confidential Data Privacy Agreement (“**DPA**”) is entered into by and between:

THE BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY, a political subdivision of the Commonwealth of Kentucky, with its principal place of business at 3332 Newburg Road, Louisville, Kentucky 40218 (the “**Board**” or “**Jefferson County Public Schools**”) and

Public Consulting Group LLC, a limited liability company in Boston, Massachusetts organized under the laws of Delaware with its principal place of business located at 148 State Street, Boston, MA 02109 (the “**Provider**”).

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

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

WHEREAS, the Provider and the Board 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, the Board and Provider agree as follows:

ARTICLE I: PURPOSE AND SCOPE

- 1. Entire Agreement.** This DPA is the entire agreement between the Parties and supersedes any and all agreements, representations, and negotiations, either oral or written, between the Parties before the effective date of this DPA. This DPA may not be amended or modified except in writing as provided below. This DPA is supplemented by the Board’s Procurement Regulations currently in effect (hereinafter “**Regulations**”) that are incorporated by reference into and made part of this DPA. In the event of a conflict between any provision of this DPA and the Regulations, the Regulations shall prevail. 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.
- 2. Term.** This DPA shall be effective as of September 15, 2025, (the “**Effective Date**”) and shall continue for three (3) years, terminating on September 14, 2028.
- 3. Services.** The services to be provided by Provider to the Board pursuant to this DPA are detailed in **Exhibit “A”** (the “**Services**”). Any compensation to be provided by the Board to Provider is also detailed in **Exhibit “A”** (the “**Compensation**”). Each party shall be responsible for their portion of costs that may result from data sharing. Examples of potential costs to the Board are costs associated with the compiling of Confidential Data requested under this DPA and costs associated with the electronic delivery of Confidential data to Provider.
- 4. Purpose of DPA.** The purpose of this DPA is to describe the duties and responsibilities to protect Confidential 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 Board. Provider shall be under the direct control and supervision of the Board, with respect to its use of Confidential Data.

5. **Confidential Data to Be Provided.** In order to perform the Services described above, the Board shall provide Confidential Data as identified in the Schedule of Data, attached hereto as **Exhibit “B”**.
6. **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.
7. **Additional Terms and Conditions.** The additional terms and conditions included in **Exhibit “F”** are incorporated into and a part of this DPA, provided that in the event of any conflict between the terms and conditions of the DPA and Exhibit F, those herein would prevail.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Confidential Data Property of the Board.** All Confidential 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 Board. The Provider further acknowledges and agrees that all copies of such Confidential 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 Confidential Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Confidential Data contemplated per the Service Agreement, shall remain the exclusive property of the Board. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the Board as it pertains to the use of Confidential Data, notwithstanding the above.
2. **Parent Access.** To the extent required by law the Board shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Confidential 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 the Board to respond to a parent or student, whichever is sooner) to the Board’s request for Confidential 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 Confidential Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the Board, 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 Board, transfer, or provide a mechanism for the Board 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 Confidential Data held by the Provider pursuant to the Services, the Provider shall notify the Board in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the Board 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 Confidential Data in a manner no less stringent than the terms of this DPA.
6. **Research and Program Evaluation.** For any project, involving data collection or research (e.g., program evaluation or monitoring activities), student or staff participation is voluntary. As a federally authorized Institutional Review Board (IRB), the Board complies with the federal definition for research, which includes sharing of Personally Identifiable Information (PII) for the purposes of answering a question or evaluating activities for effectiveness beyond standard educational or operational procedures. Thus, all data collection and research activities must be approved by the Board's IRB and shall not begin before approval is secured from the IRB. If Provider wishes to collect data specifically for program evaluation or research purposes, or if Provider wishes to use identifiable data for program evaluation or research purposes, Provider must apply for and obtain permission from the Board's IRB prior to beginning any research or evaluation related data collection.

ARTICLE III: DUTIES OF THE BOARD

1. **Provide Data in Compliance with Applicable Laws.** The Board shall provide Confidential 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 Board has a policy of disclosing Education Records and/or Confidential Data under FERPA (34 CFR § 99.31(a)(1)), the Board 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.** The Board shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Confidential Data.
4. **Unauthorized Access Notification.** The Board shall notify Provider promptly of any known unauthorized access. The Board will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance.** The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Confidential Data privacy and security, all as may be amended from time to time, including but not limited to FERPA; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq.; the Child Nutrition Act of 1966, 42 U.S.C. 1771 et seq.; 7 C.F.R. 245.6 et seq.; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; and the Kentucky Open Records Act, KRS 61.820 et seq.
2. **Data Custodian.** For the purposes of this DPA and ensuring Provider's compliance with the terms of this DPA and all application of state and federal law, Provider designated Michael Bedford as the data custodian ("Data Custodian") of the Confidential Data. The Board will release all data and information under this DPA to Data Custodian. Data Custodian shall be responsible for transmitting all data requests and maintain a log or other record of all data

requested and received pursuant to this DPA, including confirmation of the return or destruction of data as described below. The Board may, upon request, review the records Provider is required to keep under this DPA.

3. **Authorized Use.** The Confidential 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. Provider will not contact the individuals included in the data sets without obtaining advance written authorization from the Board.
4. **Provider Employee Obligation.** Provider shall require all of Provider's employees and agents who have access to Confidential Data to comply with all applicable provisions of this DPA with respect to the Confidential Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Confidential Data pursuant to the Service Agreement.
5. **No Disclosure.** Provider acknowledges and agrees that it shall not make any re-disclosure of any Confidential Data or any portion thereof, including without limitation, user content or other nonpublic information and/or personally identifiable information contained in the Confidential Data other than as required by law or court order. If Provider becomes legally compelled to disclose any Confidential Data (whether by judicial or administrative order, applicable law, rule, regulation, or otherwise), then Provider shall use all reasonable efforts to provide the Board with prior notice before disclosure (provided such notice is allowed by law) so that the Board may seek a protective order or other appropriate remedy to present the disclosure or to ensure the Board's compliance with the confidentiality requirements of federal or state law. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Confidential Data to any third party.
6. **De-Identified Data:** Provider agrees not to attempt to re-identify De-Identified Confidential Data. De-Identified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the Board 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 the Board to return or destroy Confidential Data. Except for Subprocessors, Provider agrees not to transfer de-identified Confidential 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 Board who has provided prior written consent for such transfer. Prior to publishing any document that names the Board explicitly or indirectly, the Provider shall obtain the Board's prior written approval.
7. **Disposition of Data.** Upon written request from the Board, Provider shall dispose of or provide a mechanism for the Board to transfer Confidential Data obtained under the Service Agreement in a usable format, 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 Board is received to return the data in a usable format, Provider shall dispose of all Confidential Data after providing the Board with reasonable prior notice. The duty to dispose of Confidential Data shall not extend to Confidential Data that had been De-Identified or placed in a

separate student account pursuant to section II 3. The JCPS may employ a **“Directive for Disposition of Data”** form, a copy of which is attached hereto as **Exhibit “D”**. If the JCPS and Provider employ **Exhibit “D”**, no further written request or notice is required on the part of either party prior to the disposition of Confidential Data described in **Exhibit “D”**.

8. **Advertising Limitations.** Provider is prohibited from using, disclosing, or selling Confidential 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 the Board. This section does not prohibit Provider from using Confidential Data (i) for adaptive Learning or customized student Learning (including generating personalized Learning recommendations); or (ii) to make product recommendations to teachers or JCPS employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Confidential Data as permitted in this DPA and its accompanying exhibits.
9. **Liability.** Provider agrees to be responsible for and assumes all liability for any claims, costs, damages or expenses (including reasonable attorneys’ fees) that may arise from or relate to Provider’s intentional or negligent release of personally identifiable student, parent or staff data (“Claim” or “Claims”). Provider agrees to hold harmless the Board and pay any costs incurred by the Board in connection with any Claim. The provisions of this Section shall survive the termination or expiration of this DPA.

ARTICLE V: DATA PROVISIONS

1. **Data Storage.** Where required by applicable law, Confidential Data shall be stored within the United States. Upon request of the Board, Provider will provide a list of the locations where Confidential Data is stored.
2. **Audits.** No more than once a year, or following unauthorized access, upon receipt of a written request from the Board with at least ten (10) business days’ notice and upon the execution of an appropriate confidentiality agreement, the Provider will allow the Board to audit the security and privacy measures that are in place to ensure protection of Confidential Data or any portion thereof as it pertains to the delivery of services to the JCPS . The Provider will cooperate reasonably with the Board 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 the Board, and shall provide reasonable access to the Provider’s facilities, staff, agents and the Board’s Confidential Data and all records pertaining to the Provider, the Board and delivery of Services to the Board. 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 Confidential 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 standards set forth in **Exhibit “E”**. Additionally, Provider may choose to further detail its security programs and measures that augment or are in addition to the Cybersecurity Framework in **Exhibit “E”**. Provider shall provide, in the Standard Schedule to the DPA, contact information of an employee who the Board may contact if there are any data security concerns or questions. Additionally, The Provider agrees to maintain a minimum security standard including but limited to the following precautions and protections:

- a) Encrypting all data, at rest and in transit;
- b) Maintaining multi-factor authentication on accounts that can access the network or email remotely, including 3rd party accounts;
- c) Securing access to any physical areas/electronic devices where sensitive data are stored;
- d) Establishing and enforcing well-defined data privilege rights which follow the rule of least privilege and restrict users' access to the data necessary for this to perform their job functions;
- e) Ensuring all staff and 3rd parties sign a nondisclosure statement, and maintaining copies of the signed statements;
- f) Installing end-point protection including but not limited to anti-malware and anti-spyware on any device connected to the network that has access to scoped data, when applicable

4. **Data Breach.** In the event of an unauthorized release, disclosure or acquisition of Confidential Data that compromises the security, confidentiality or integrity of the Confidential Data maintained by the Provider the Provider shall provide notification to the Board 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 individual reporting a breach subject to this section.
 - ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
 - iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and
 - v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
- (2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Confidential 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 Confidential Data or any portion thereof, including personally

identifiable information and agrees to provide the Board, upon request, with a summary of said written incident response plan.

- (4) The Board shall provide notice and facts surrounding the breach to the affected students, parents or guardians, or staff, as applicable.
- (5) In the event of a breach originating from the Board's use of the Service, Provider shall cooperate with the Board to the extent necessary to expeditiously secure Confidential Data.

5. Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act.

If Provider receives Personal Information as defined by and in accordance with the Kentucky Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, et seq. (the "Act"), Provider shall secure, protect and maintain the confidentiality of the Personal Information by, without limitation, complying with all requirements applicable to "non-affiliated third parties" set forth in the Act, including but not limited to the following:

- a. "Personal Information" is defined in accordance with KRS 61.931(6) as an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:
 - i. An account, credit card number, or debit card number that, in combination with any required security code, access code or password, would permit access to an account;
 - ii. A Social Security number;
 - iii. A taxpayer identification number that incorporates a Social Security number;
 - iv. A driver's license number, state identification card number or other individual identification number issued by an agency;
 - v. A passport number or other identification number issued by the United States government; or
 - vi. Individually Identifiable Information as defined in 45 C.F.R. sec. 160.013 (of the Health Insurance Portability and Accountability Act), except for education records covered by FERPA.
- b. As provided in KRS 61.931(5), a "non-affiliated third party" means any person or entity that has a contract or agreement with an agency and receives (accesses, collects or maintains) personal information from the agency pursuant to the contract or agreement.
- c. Provider shall not re-disclose, without the written consent of JCPS, any "personal information," as defined in KRS 61.931, or any other personally identifiable information of a student or other persons, such as employees.
- d. Provider agrees to cooperate with JCPS in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

- e. Provider agrees to undertake a prompt and reasonable investigation of any breach as required by KRS 61.933.

6. Cloud Computing Service Providers. If Provider is a cloud computing service provider (as defined in KRS 365.734(1)(b) as "any person other than an educational institution that operates a cloud computing service"), Provider agrees that:

Provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. Provider shall work with the student's school and district to determine the best method of collecting parental permission. KRS 365.734 defines "process" and "student data."

Pursuant to KRS 365.734(2), Provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purposes.

Pursuant to KRS 365.734(2), Provider shall not sell, disclose, or otherwise process student data for any commercial purpose.

Pursuant to KRS 365.734(3), Provider shall certify in writing to the agency that it will comply with KRS 365.734(2).

ARTICLE VI: MISCELLANEOUS

1. **Termination.** Either party may terminate this DPA if the other party breaches any terms of this DPA, provided however, the breaching party shall have thirty (30) days to cure such breach and this DPA shall remain in force. The Board may terminate this DPA in whole or in part at any time by giving written notice to Provider of such termination and specifying the effective date thereof, at least thirty (30) days before the specified effective date. In accordance with **Attachment A**, the Board shall compensate Provider for Services satisfactorily performed through the effective date of termination.
2. **Effect of Termination Survival.** If the Service Agreement is terminated, the Provider shall destroy all of JCPS's Confidential Data pursuant to Article IV, section 6.
3. **Priority of Agreements.** This DPA shall govern the treatment of Confidential 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.
4. **Modification.** No waiver, alteration or modification of the provisions of this Agreement shall be binding unless in writing and mutually agreed upon. Any modifications or additions to this Agreement must be negotiated and approved by both parties.
5. **Disputes.** Any differences or disagreements arising between the Parties concerning the rights or liabilities under this DPA, or any modifying instrument entered into pursuant to this DPA, shall be resolved through the procedures set out in the Regulations.

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

The designated representative for the Board for this DPA is:

Name: Eric Satterly _____

Title: Chief Information Officer

Address: 3332 Newburg Road, Louisville, KY 40218 _____

Phone: 502-485-3485 _____

Email:eric.satterly@jefferson.kyschools.us

The designated representative for the Provider for this DPA is:

Name: Robbie Ammons Title: _____

Address:140 Mariners Cay Rocky Point, NC 28457

Phone: 704-839-6281 _____ Email:

7. **Amendment and Waiver.** 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.
8. **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.
9. **Governing Law; Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE COMMONWEALTH OF KENTUCKY, 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 JEFFERSON COUNTY KENTUCKY FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

- 10. 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 Board 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 Confidential Data within the Service Agreement. The Board 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.
- 11. Authority.** Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Confidential Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Confidential Data and/or any portion thereof.
- 12. Relationship of Parties.** The Board is not an employee, agent, partner or co-venturer of or with Services Provider. Neither Services Provider nor the Board shall represent or imply to any party that it has the power or authority to enter into a contract or commitment in the name of or on behalf of the other, or to otherwise bind the other.
- 13. Equal Opportunity.** During the performance of this DPA, Provider agrees that Provider shall not discriminate against any employee, applicant or subcontractor because of race, color, national origin, age, religion, marital or parental status, political affiliations or beliefs, sex, sexual orientation, gender identity, gender expression, veteran status, genetic information, disability, or limitations related to pregnancy, childbirth, or related medical conditions. If the Compensation is paid from federal funds, this DPA is subject to Executive Order 11246 of September 24, 1965 and in such event the Equal Opportunity Clause set forth in 41 Code of Federal Regulations 60-1.4 is hereby incorporated by reference into this DPA as if set forth in full herein.
- 14. Prohibition on Conflicts of Interest.** It shall be a breach of this DPA for Provider to commit any act which is a violation of Article XI of the Regulations entitled "Ethics and Standards of Conduct," or to assist or participate in or knowingly benefit from any act by any employee of the Board which is a violation of such provisions.
- 15.** Contractor shall be in continuous compliance with the provisions of KRS Chapters 136, 139, 141, 337, 338, 341, and 342 that apply to Provider for the duration of this DPA and shall reveal any final determination of a violation by the Provider of the preceding KRS chapters.
- 16. Access to School Grounds.** No employee or agent of Provider shall access the Board's school grounds on a regularly scheduled or continuing basis for purposes of providing services to students under this DPA.

IN WITNESS WHEREOF, The Board and Provider execute this DPA as of the Effective Date above.

BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY

By: _____ Date: _____

Printed Name: Dr. Brian H. Yearwood

Title/Position: Superintendent

PUBLIC CONSULTING GROUP LLC By: Robbie Ammons



_____ Date:02/10/2026 _____

Printed Name:Robbie Ammons _____

Title/Position:Manager _____

EXHIBIT "A"

DESCRIPTION OF SERVICES

Provider shall provide software licenses and support for the following products at prices equal or below Provider's standard pricing rates for the products:

This Exhibit A is used to document the base EDPlan modules, features, and service levels that the Board (or in this Exhibit "School System") has elected to license/purchase under this Agreement. Additional services are described within this Exhibit A to facilitate meeting future district needs should School System choose to exercise additional related contract options at a later point in time.

PCG deploys a standard configuration of EDPlan to School Systems, informed by industry best practice. For each new implementation of any EDPlan module, PCG will hold a kickoff meeting with the designated School System contract manager to discuss implementation and configuration options that are available to School System.

In addition to licensing access to the EDPlan service to School System, PCG offers a number of professional services for School Systems that may include: user help desk support regarding system functions and operation; a variety of tiered technical assistance levels to support related to school operations, policy, and instruction; related online and in-person professional development; and other related services.

For on-site trainings, School System is responsible for scheduling the space, providing necessary technology (computers/Internet), and communicating/promoting the details of the event to School System personnel.

Subject to the terms and conditions of the Agreement, PCG will provide the EDPlan™ Service as follows:

EDPlan Modules and Functionality Licensing and Access

- **EDPlan Behavioral Threat Assessment and Management Solution.** *PCG's Behavioral Threat Assessment and Management (BTAM) solution assists in the implementation of a consistent, structured approach for multidisciplinary teams to identify and support students who may present a threat to self or others; helping school personnel document the threat, gather, share, and consider relevant information to make informed decisions, consider key questions to assign risk and determine next steps for intervention, and prepare a monitoring plan if needed).*
 - Includes standard configurations supporting local and national models.
 - PCG will provide:
 - EDPlan Systems Annual Refresher Training – Includes one (1) 2-hour virtual refresher training session per contract year. Additional training sessions can be requested for an additional cost.
 - Free 90-day trial of online training modules developed by national threat assessment expert Dr. Melissa Reeves based on the NTAC model; and John Van Dreal based on the SK Cascade model; both one seat license.
 - The package further includes:
 - Advanced Reporting (AR): Flexible enterprise-scale ad-hoc reports.
 - Five (5) standard AR reports

- Two (2) hours of virtual training on AR
 - Additional reports provided at published rates in Exhibit B
 - Standard edition EDPlan PaperClip: Document Repository for BTAM case artifacts.
 - File types supported: PDF, DOC, XLS, TXT, RTF, PPT, TIF, JPG, PNG, XLSX, PPTX, and DOCX.
- **Suicide Risk Assessment Solution.** *The Suicide Prevention (SRA) solution works to prompt users through Threat-to-Self risk assessment using commonly used screeners. A safety and support supervision plan with recommended interventions is created and monitored for the individual student.*
- The SRA solution includes PCG’s standard configuration that supports local and national models.
- In the first year of service, PCG will provide:
 - One (1) day of expert PCG consultant training integrated with district practice – Two (2) sessions per day and 30 participants per session. BTAM/SRA teams and district administrators will learn how to navigate the EDPlan system and manage threat/risk assessment data with 2 expert PCG trainers.
 - EDPlan Systems Annual Refresher Training – Includes one (1) 2-hour virtual refresher training session per year.
 - Additional training sessions can be requested for an additional cost.
 - Free 90-day trial of online training modules developed by national suicide risk assessment expert Dr. Terri Erbacher based on the Suicide in Schools model; one seat license.
- The package further includes:
 - Advanced Reporting (AR): Flexible enterprise-scale ad-hoc reports.
 - Five (5) standard AR reports
 - Two (2) hours of virtual training on AR
 - Additional reports provided at published rates in Exhibit B
 - Standard edition PaperClip: Document Repository for BTAM case artifacts.
 - File types supported: PDF, DOC, XLS, TXT, RTF, PPT, TIF, JPG, PNG, XLSX, PPTX, and DOCX.

User Support

□ Standard User Support – EDPlan Functionality and Feature Support (included in Service Agreement)

EDPlan was designed to be intuitive and to facilitate ease of use. Licensing fees include user support related solely to specific functionality and system features that are included in this Agreement. In addition to the Main Menu Resource Information section on the EDPlan Dashboard, where users can find system documentation and FAQs, PCG provides live support on basic system functions. User Support includes communication tools integrated within the EDPlan user interface, a dedicated email address (utahedplan@pcgus.com), and a telephone hotline (385-203-8562). PCG will respond to user inquiries within one business day. Items that are escalated for additional investigation or resolution may take additional time to resolve.

Integrated Communication Tool: School System can send inquiries and support requests via EDPlan. PCG will respond within one business day.

Email: Only School System designated Project Manager or Contract Manager will be authorized to contact PCG via utahedplan@pcgus.com. PCG will respond to School System inquiries and support requests via utahedplan@pcgus.com within one business day.

Telephone: Only School System designated Project Manager or Contract Manager will be authorized to contact PCG via the call center. Those persons should only contact the call center if the request is urgent. By limiting calls to urgent matters, PCG can provide a more immediate response to School System. All non-urgent requests should be entered via the EDPlan web-based application or sent to PCG via utahedplan@pcgus.com. The call center is available Monday through Friday from 9:00AM – 5:00PM MST, with the exception of PCG holidays. School System will have an initial 50 calls to the call center available for the school year. Once the 50 calls are completed, School System can schedule additional trainings or purchase an additional block of 50 calls. Please see Exhibit B for costs and terms.

Supplemental Program and Department Support

Supplemental Program and Department Support is beyond the Functionality and Feature Support included in the licensing fee. This supplemental tier of support is available for an additional fee if purchased by School System and includes inquiries related to School System safety operations, policies, procedures, or compliance.

Supplemental Program and Department Support is requested by phone and email only, must be scheduled at least 5 business days in advance, and can be purchased in banks of 10 hours at a rate of \$4,250 for each 10-hour bank.

In cases where this supplemental support has not been purchased by School System, any inquiries related to School System special education policy, procedures, or operations support services and state or federal laws, regulations, or administrative code will be referred to back to School System. PCG DOES NOT PROVIDE ANY LEGAL ADVICE NOR SHOULD ANY SERVICE IT PROVIDES BE CONSTRUED AS PROVIDING LEGAL ADVICE. SCHOOL SYSTEM SHOULD CONSULT WITH ITS LEGAL COUNSEL WHEN NECESSARY.

Supplemental Services- Basic and Advanced Data Analysis and Custom Reporting Services

Requests for Data Analysis and custom reporting services must be submitted via the EDPlan Help Desk. PCG will acknowledge receipt within one business day. These services require additional fees as indicated in Exhibit B.

System Overview and School System Responsibilities

EDPlan is a web-based application. School System is not required to purchase or install any software on its computers except an Internet browser and Adobe Reader (each is available from the vendor).

PCG provides all hardware and software necessary for the operation of EDPlan. PCG provides all technology engineering services required to operate EDPlan. PCG provides all operational services needed for the appropriate functioning of EDPlan including but not limited to: database software administration, database backup and recovery, system account management, system security, computer and network equipment maintenance, server software maintenance, application software maintenance. PCG provides all datacenter hosting services as required for the appropriate functioning of EDPlan, including the provisioning of internet bandwidth as needed to make EDPlan appropriately accessible via the internet.

School System Responsibilities

School System is responsible for timely provision of the following:

1. Connection to the Internet for its Users
2. Computer hardware for its Users
3. Browser software and browser software configuration
4. Installation and configuration of the Adobe Acrobat Reader
5. System start-up information as detailed in the “System Start-Up” Section below
6. Additional school data after start-up, as may be required by PCG
7. Access to Special Education management staff
8. Designation of a consistent project manager who will serve for the duration of the project term. In case of transition of staff
9. Scheduling as needed to allow the project manager to receive training from PCG on an ongoing basis
10. Sites for all scheduled trainings with an appropriately configured computer for each trainee and one additional computer for the trainer

System Integration

Standard System Integration

System Integration is a step in the initial implementation phase. The goal of System Integration is to establish flow of student demographic information into EDPlan, with School System’s Student Information System serving as the primary source of data. PCG will work with School System, using established PCG processes and templates, to implement the initial System Integration configuration through which data will be exchanged on a nightly basis within PCG’s overnight schedule and one student information system. PCG assumes that School System will actively participate in the process, and that School System has current technology and security protocols in place to help create and maintain a strong security posture with respect to this integration. School System data housed in systems other than the single student information system may be integrated at additional fees.

PCG has developed a standard set of specifications to outline the data elements required from School System’s local data systems by PCG to properly configure EDPlan. This includes the following five (5) elements:

- Student Information
- Parent Information
- User Information
- School Information
- Caseload Information

School System Responsibilities

PCG will assist School System in populating the spreadsheet templates provided by offering technical advice and consulting, but it is the responsibility of School System to populate the spreadsheets and to submit those to PCG personnel via secure file transfer protocols which will be described to School System personnel who are preparing and delivering the data.

COMPENSATION

Purchase orders shall be entered by each participating school. Funds for purchase shall come from individual school budgets. Total payments under this DPA shall not exceed \$ 174,000.00 per fiscal year, running from July 1-June 30, with up to a 3% increase in cost per year in the 26-27 and 27-28 fiscal year.

Subject to the terms and conditions of this Agreement, the Board shall pay PCG the following amounts:

Pricing	September 15, 2025 – September 14, 2026
EDPlan BTAM Solution	\$135,000
Invoice Submission	September 30, 2025
Professional Development	\$20,000
Invoiced as delivered	
Hourly Consulting Rate	\$425 per hour for blocks up to 3 hours (after which daily rate applies)
Invoiced as delivered	
Hourly Software Development Rate	\$210 per hour
Invoiced as delivered	

A. Fees

- Total fees will not exceed \$174,000 per contract year.
- For each Renewal Term of the Agreement commencing on September 15, 2026, School System shall pay an Annual Fee equal to 103% of the amount of the Annual Fee for the previous Initial or Renewal Term.
- Professional Development of \$20,000 provides up to 4 onsite or virtual days of consultation.
- Hourly Software Development Rate of \$210 per hour applies to mutually agreed hours of design, programming, testing, and deployment of Jefferson County specific customizations, which agreement is memorialized in writing (e-mail being sufficient).

B. Additional Fees

The parties will negotiate in good faith concerning fees for additional training, features, or additional work under this Agreement that are not otherwise stated herein. Once the parties reach agreement, the fees will be memorialized through amendments to this Agreement. School System reserves the right to procure additional solutions and services from PCG. It is understood that these additional solutions and services are not included in scope of this Agreement and do not include training or installation costs for additional scope. In instances where pricing has previously been provided to School System, PCG will honor those prices for a period of 120 days.

- In-person professional development with a national certified trainer \$6000 per day plus expenses

- Formally approved system changes and modifications may be purchased: \$210/development hour (Development Hours constitute design, development, and testing of requested change)
- Two additional three-hour sessions, on the same day, of Standard On-Site Training for up to 30 School System staff members per session with two PCG trainers: \$6000
- Virtual Training: two three-hour training sessions at \$1500
- Data analysis, custom data feeds, or custom report development: \$220/hour
- Policy or procedure analysis and guidance with PCG subject matter experts: \$300/hour
- Additional annual subscriptions for unlimited online professional development modules for Suicide in Schools with Dr. Terri Erbacher, or NTAC with Dr. Melissa Reeves, or Salem-Keizer Cascade with John Van Dreal, or other threat model domains are \$250 per school per School System per topic.

EXHIBIT "B"
SCHEDULE OF DATA

Category of Data	Elements	Check if Used by Your System (Windows)	Check if Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check if Used by Your System (IOS)	Check if Used by Your System (Browser Based)	Check If Used by Your System (Other, please specify: _____)
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Other application technology meta data- Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Assessment Some assessment data may be entered into service logs for students by those performing the assessments.	Standardized test scores	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Communications	Online communications captured (emails, blog entries)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Demographics	Date of Birth	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Place of Birth	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Gender	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Language information (native, or primary language spoken by student)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Category of Data	Elements	Check if Used by Your System (Windows)	Check if Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check if Used by Your System (iOS)	Check if Used by Your System (Browser Based)	Check if Used by Your System (Other, please specify: _____)
	Other demographic information-Please specify: See attached existing DPA for detailed list of additional data.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enrollment	Student school enrollment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student grade level	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Homeroom	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Phone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Special Indicator	English language Learner Information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Low Income status	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Medical alerts/ health data Service logs containing health data will be entered. See attached existing DPA agreement for more details.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Category of Data	Elements	Check If Used by Your System (Windows)	Check If Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check If Used by Your System (iOS)	Check If Used by Your System (Browser Based)	Check if Used by Your System (Other, please specify: _____)
	Specialized education services (IEP or 504)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Staff Data	First and Last Name	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Email Address	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Staff ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Other information – Please specify License information for health providers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student Contact Information	Address	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Email	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Phone	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	State ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Provider/App assigned student ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program- student types 60 wpm, reading program- student reads below grade level)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Student work	Student generated content; writing, pictures, etc.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Category of Data	Elements	Check If Used by Your System (Windows)	Check If Used by Your System (ChromeOS - apps/extensions from Chrome Web Store and Google Play Store)	Check If Used by Your System (IOS)	Check If Used by Your System (Browser Based)	Check if Used by Your System (Other, please specify: _____)
	Other student work data -Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student course grades/ performance scores	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Other transcript data - Please specify:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Transportation	Student bus assignment	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Student bus card ID number	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Other transportation data – Please specify: The existing DPA agreement is attached. All of the currently approved data will continue to be shared.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other	Please list each additional data element used, stored, or collected by your application: The existing DPA agreement is attached. All of the currently approved data will continue to be shared.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
None	No Confidential Data collected at this time. Provider will immediately notify JCPS if this designation is no longer applicable.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

EXHIBIT “C”
DEFINITIONS

Compensation: Amounts to be paid to the Provider in exchange for software licenses and support. The maximum amount of Compensation that may be paid under this DPA is set forth in Attachment A. The Board is not obligated to pay the maximum Compensation amount solely by its inclusion in this DPA. Compensation owed is determined by the purchase orders submitted to Provider. The cost for any single license or support provided under this DPA shall not exceed Provider’s standard pricing for that product.

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 the Board to provide a service to the Board shall be considered an “operator” for the purposes of this section.

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 Confidential Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Regulations: The Board Procurement Regulations, available on the JCPS website, as may be amended from time to time.

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 Confidential 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.

Confidential Data: Confidential Data includes any data, whether gathered by Provider or provided by the Board 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. Confidential Data includes Meta Data. Confidential Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Confidential Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Confidential Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Confidential 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 Board 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 Confidential Data.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Confidential 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 Confidential 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

The Board of Education of Jefferson County Kentucky directs Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between The Board and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

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

[Insert categories of data here]

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

2. Nature of Disposition

_____ Disposition shall be by destruction or deletion of data.

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

[Insert or attach special instructions]

3. Schedule of Disposition

Data shall be disposed of by the following date:

_____ As soon as commercially practicable.

_____ By **[Insert Date]**

Signature

Authorized Representative of the Board

Date

Verification of Disposition of Data

Authorized Representative of Provider

Date

EXHIBIT “E”

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

Provider will utilize one of the following known and credible cybersecurity frameworks which can protect digital learning ecosystems.

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	FRAMEWORK(S)
X	American Institute of CPAs	SOC2
	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	The Board of Education of Jefferson County	Board provided standardized questionnaire

EXHIBIT "F"**ADDITIONAL EDPLAN™ BTAM LICENSE TERMS AND CONDITIONS**

WHEREAS, PCG desires to license to the Board PCG's proprietary Internet-based education case management, document creation, and supporting analytics software (EDPlan™) module to assist administrators and school-based threat assessment teams with the documentation, communication, and monitoring requirements of behavioral threat assessments and management and suicide risk assessments (BTAM Solution), and to license PCG's related proprietary systems and documentation; and

WHEREAS, the Board desires to provide the EDPlan BTAM Solution to its school and administrative employees, contractors, and authorized users for their use in the creation of behavioral threat assessments and monitoring plans; and

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. "Application Management" means work related to how the EDPlan Service is modified, and includes resolving defects, updating the EDPlan Service for PCG system-wide national releases to the base product rolled out on a predefined quarterly schedule, processing change requests to modify/change the EDPlan Service, release schedules/processes, testing processes, and acceptance processes.

1.2. "Confidential Information" means information designated or treated as confidential by either party, or which under the circumstances surrounding disclosure should in good faith be treated as confidential, including but not limited to: (a) computer programs, electronic codes, algorithms, know-how, formulas, processes, ideas, data, inventions (whether or not subject to patent or copyright), schematics, teaching and development techniques, trade secrets, improvements, research projects, and code; (b) information about costs, profits, markets, sales, customers, or clients; (c) technical, business, and financial plans; (d) employee personnel files and compensation information; (e) discoveries, developments, designs, improvements, regardless of the form of communication in each case, including extracts or summaries; and (f) any record (whether in print, electronic, or any other medium) maintained by Board, a Board employee or agent, or a party acting on Board's behalf, which is directly related to an identified student. "Confidential Information" also specifically includes the EDPlan Service, any third-party information disclosed to either party under obligations of confidentiality, and the identity of or any medical, financial, or personal information pertaining to anyone within PCG or Board provided that PCG shall be permitted to disclose education records to any subcontractor or vendor which is bound by confidentiality and data security requirements for the exclusive purpose of supporting the provision of services under this Agreement. Notwithstanding the foregoing, however, "Confidential Information" does not include information that: (i) was rightfully in possession of or known to the receiving party without any obligation of confidentiality prior to receiving it from the disclosing party; (ii) is, or subsequently becomes, legally and publicly available without breach of this Agreement; (iii) is rightfully obtained by the receiving party from a source other than the disclosing party without any obligation of confidentiality; or (iv) is disclosed by the receiving party under a valid order of a court or government agency, provided that the receiving party provides prior written notice to the disclosing party of such obligation and the opportunity to oppose such disclosure.

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

1.4. "EDPlan Service" means: (i) the implementation of the Internet-based functionality of EDPlan modules identified in this Agreement; (ii) licenses for the EDPlan modules specifically identified in this Agreement; (iii) all products and work related to such services within this Agreement, including but not limited to Playbook; (iv) Production Support for the implemented EDPlan modules; and (v) the Documentation developed by PCG for distribution and use in combination with the foregoing.

1.5. “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.

1.6. “Production Support” means ongoing operations and services to maintain user support of the EDPlan Service following activation of the EDPlan Service in the production environment, including work related to resolving unplanned system outages, work related to keeping the EDPlan Service in tune and running properly, i.e., hosting, operating system updates, up time, and maintenance schedules (system unavailability), and Application Management.

1.7. “Board User” means any employee, contractor, and other authorized user of the “Board” who will be granted access to the EDPlan Service, provided that such contractors or other non-employees are subject to terms and conditions concerning confidentiality of licensing that are materially similar to those set forth herein.

1.8. “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.

2. EDPLAN™ SERVICE. Subject to the terms and conditions of this Agreement, including Board’s performance of its obligations hereunder, PCG shall provide access to the EDPlan Service to Board.

2.1. Grant of License for EDPlan Service. PCG grants to the Board, and the Board accepts, a non-exclusive, non-transferable, non-sublicensable, and revocable 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 Board, and the Board accepts, a non-exclusive, non-transferable, non-sublicensable, and revocable royalty-free license under PCG’s copyrights in PCG’s Documentation, during the Term only to (i) incorporate PCG’s Documentation, in whole or in part, into other written materials prepared by or for the Board with respect to the EDPlan Service; and (ii) reproduce and distribute modified and original versions of PCG’s Documentation, in hard copy or in an online format, as part of the Board’s Documentation for the EDPlan Service, and, if such Board’s Documentation is in an online format, allow Board Users to make print copies of the same.

2.3. Restrictions on License Grant. Unless expressly authorized by this Agreement or in writing by PCG:

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

2.3.2. The Board shall ensure that appropriate proprietary notices indicating PCG’s Intellectual Property Rights in the EDPlan Service and related Documentation are placed on all copies of written materials distributed by the Board relating thereto. Examples of such documentation include training materials and manuals. The Board 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 Board User or third party to do so.

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

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

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

2.3.6. The Board shall not circumvent any security protection within the EDPlan Service, and shall not permit any Board User or third party (e.g. other vendors or consultants) to do so.

2.4. Reservation of Rights. Subject to the license rights granted to the Board 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 the Board 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 Documentation or Trademarks. Except as expressly authorized by this Agreement, the Board shall not use, display, copy, distribute, modify, or sublicense the EDPlan Service. PCG reserves all rights not expressly granted to the Board by this Agreement.

3. ACCESS TO EDPLAN. PCG will provide access to the EDPlan web-based application to the Board. PCG does not provide Internet connectivity to The Board, and obtaining and maintaining such connectivity will be the sole responsibility of The Board.

4. WARRANTIES

4.1. 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 the Board'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 or emergency maintenance of the EDPlan Service, the scheduled maintenance of PCG's Internet provider, or any force majeure event, shall not be deemed a failure to provide the EDPlan Service.

4.2. BTAM SOLUTION. Note that PCG's BTAM solution is a set of tools to be used by The Board'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 provide the Board'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 BTAM solution should not be construed as determining actions or decisions upon which The Board must or should rely

4.3. DISCLAIMER. PCG specifically disclaims any other warranties, whether written or oral, expressed or implied, with respect to the EDPlan products or related services provided by PCG under this Agreement, including any implied warranties or merchantability or fitness for a particular purpose.

5. PROPRIETARY RIGHTS; PROTECTION OF CONFIDENTIAL INFORMATION

5.1. Ownership. The Board 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 the Board owns all of the data inputted by each Board User for purposes of creating a plan and any and all reports produced as a result of using the EDPlan Service during the Agreement term. The Board acknowledges that for PCG's own purposes PCG shall have the right to aggregate any data input by the Board or Board Users, but PCG shall not use or disclose personal or individual identifying information where the use or disclosure would constitute a breach of a known privacy policy adopted by either PCG or the Board.

5.2. The Board Duties. The Board 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 The Board becomes aware. The Board 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 Board Users. The Board is responsible for establishing and enforcing any The Board policies related to data security, information management, account management of Board Users, and the proper handling of data extracted, reported, or otherwise removed by the system by The Board personnel.

5.3. PCG Duties. PCG will take reasonable steps to protect the data that the Board 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 Board data is the property of the Board. Upon termination or expiration of this Agreement and for a limited period of no more than thirty (30) days, or at the Board's request, PCG will provide access to all data to the Board. A fee equal to PCG's standard hourly rates will apply if The Board requests PCG to download and transmit the data to the Board. Notwithstanding anything to the contrary in this Agreement, PCG may keep a backup copy of the data unless otherwise agreed by the parties, subject to applicable law.

5.4. 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.

5.5. Legal Obligation. Nothing in this Agreement prohibits a party from disclosing Confidential Information pursuant to a lawful order of a court or government agency, but only to the extent of such order, and subject to such party giving prompt notice of such order to the other party so that it may seek a protective order or take other action to protect the information that was ordered to be disclosed.

6. PRODUCT MARKING. The Board 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 the Board use of the EDPlan Service with respect to PCG's Trademarks shall inure exclusively to the benefit of PCG. The Board 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 the Board's knowledge of such infringements or acts. The Board is also prohibited from altering, modifying, or creating any derivative trades names, service marks, and logos concerning EDPlan without the express written consent of PCG.

7. LIMITATION OF LIABILITY. NO PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR CONSEQUENTIAL, INCIDENTAL, EXEMPLARY, SPECIAL, OR PUNITIVE DAMAGES RESULTING FROM OR RELATING TO THE AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT, OR OTHERWISE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ADDITION, EXCEPT AS OTHERWISE PROVIDED IN THIS SECTION, THE TOTAL AGGREGATE LIABILITY OF EACH PARTY, ITS AFFILIATES, AND ALL OF ITS AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, SUBCONTRACTORS, AGENTS, SUCCESSORS

AND ASSIGNS UNDER THIS AGREEMENT (WHETHER IN CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY IN TORT, IN LAW OR EQUITY, OR OTHERWISE) SHALL NOT EXCEED, IN THE AGGREGATE, THE AMOUNT OF FEES PAID BY THE BOARD TO PCG, FOR THE SERVICE OR MODULE FROM WHICH THE LIABILITY ARISES, DURING THE TWELVE (12) MONTHS PRIOR TO THE MONTH IN WHICH THE FIRST EVENT GIVING RISE TO LIABILITY OCCURRED.