

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

Aunt Bertha, a Public Benefit Corporation organized under the laws Delaware with its principal place of business located at 3429 Executive Center Drive, Austin, TX 78731 (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 July 26, 2023 (the “**Effective Date**”) and shall continue for three (3) years, terminating on July 25, 2026.
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.

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 by Provider that remain Confidential Data, 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, provided that, as necessary in connection with the Service Agreement, to the extent that use of Confidential Data would require a license, the Board hereby automatically grants such license to Provider. 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 Chad Denton 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 except as necessary for the services 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. **Insurance.** Provider shall maintain, during the term of this Agreement, a cyber-insurance liability policy, in the amount of \$5M. Upon request, Provider shall furnish the certificate of insurance evidencing this coverage. The certificate of insurance shall name the Board of Education of Jefferson County as additional insured in the Description of Operations section of the Certificate of Insurance which shall read:

Board of Education of Jefferson County
Attn: Insurance/Real Estate Dept.
3332 Newburg Road
Louisville, Kentucky 40218

6. **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 or permitted by this DPA. 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 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.
7. **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; and (4) as agreed in the Service Agreement.

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.

8. **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"**.
9. **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 without consent 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.
10. **Intentionally omitted.**

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 by Provider.
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 at Board's cost to the Provider's facilities, staff, agents and the Board's Confidential Data and all data protection 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. 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;
- d) Ensuring all staff and 3rd parties sign a nondisclosure statement, and maintaining copies of the signed statements;
- e) 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

- i. 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.
- (1) 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.
- (2) The Board shall provide notice and facts surrounding the breach to the affected students, parents or guardians, or staff, as applicable.
- (3) 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. 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. The terms of the DPA shall be subject to the terms of the Service Agreement, provided that, 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: Dr. Eva Stone Title: Manager District Health

Address: Jefferson County Public Schools, c/o 3301 Stroble Drive, Louisville, KY 40213

Phone: 502/485-3387 Email: eva.stone@jefferson.kyschools.us

The designated representative for the Provider for this DPA is:

Name: Chad Denton Title: CFO

Address: 3429 Executive Center Drive, Austin, TX 78731

Phone: 512-717-0518 _____ Email: cdenton@findhelp.com

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.
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. **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. **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 CPA and shall reveal any final determination of a violation by the Provider of the preceding KRS chapters.**

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. Marty Pollio

Title/Position: Superintendent

AUNT BERTHA

By: Tyler Hartung _____ Date: 07/06/2023
C248E85225679E86A8CC8B014EE01495 contractworks

Printed Name: Tyler Hartung

Title/Position: VP of Finance

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:

SchoolCare is a health services and care coordination platform for customers, their employees and agents, and the parents/legal guardians of customer’s students

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 \$0 per fiscal year, running from July 1-June 30.

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	x
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	

6.23.23 - AUNT BERTHA / SCHOOLCARE

Student class attendance data

Communications	Online communications captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	x
	Place of Birth	
	Gender	x
	Ethnicity or race	
	Language information (native, or primary language spoken by student)	
	Student disability information	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	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	

Parent/Guardian Contact
Information

Address

	Email	x
	Phone	x
Parent/Guardian ID	Parent ID number (created to link parents to students)	x
Parent/Guardian Name	First and/or Last	x
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language Learner information	
	Low income status	
	Medical alerts/ health data	

Category of Data	Elements	Check if Used by Your System
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Staff Data	First and Last Name	x
	Email Address	x
	Staff ID number	
	Other information – Please specify	
Student Contact Information	Address	x
	Email	x
	Phone	x

Student Identifiers Local (School district) ID number

	State ID number	
	Provider/App assigned student ID number	x
	Student app username	x
	Student app passwords	x
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	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures, etc.	

Category of Data	Elements	Check if Used by Your System
	Other student work data -Please specify:	
Transcript	Student course grades	
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	
	Student bus card ID number	

Other transportation data – Please specify:

Other	Please list each additional data element used, stored, or collected by your application:	
None	No Confidential Data collected at this time. Provider will immediately notify JCPS if this designation is no longer applicable.	

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



SchoolCare Customer Subscription Agreement

This agreement ("Agreement") is entered into between the Customer by and between Aunt Bertha, a Public Benefit Corporation, with its headquarters located at 3429 Executive Center Drive, Suite 100, Austin, Texas 78731 ("Aunt Bertha" also doing business as "**SchoolCare**" and "**findhelp®**" and "**findhelp.org**") and **Jefferson County Public Schools** ("Customer"), located at **3332 Newburg Road, Louisville, KY 40218** for services and/or products pursuant to Exhibit A and Exhibit B attached hereto, which Exhibit A and Exhibit B are fully incorporated into the terms of this Agreement. Customer agrees to participate in parent/guardian outreach efforts to support the Care Coordination program. This Agreement will be effective (Effective Date) upon the last signature date of the below Parties. The SchoolCare platform subscription is provided at no cost to the Customer under this Agreement.

Agreed to by:

Jefferson County Public Schools (Customer)

By: _____

Name: _____

Title: _____

Date: _____

SchoolCare (Aunt Bertha)

By: 
C248E85225679E86A8CC8B014EE01495 contractworks

Name: Tyler Hartung

Title: VP of Finance

Date: 07/12/2023



(Exhibit A)

SchoolCare Services Agreement

This Services Agreement (“**Agreement**”) is made by and between the entity (“**Customer**”) identified on the attached Customer Subscription Agreement and Aunt Bertha, a Public Benefit Corporation, with its SchoolCare headquarters located at 3429 Executive Center Drive, Suite 100, Austin, Texas 78731 (“Aunt Bertha” also doing business as “**SchoolCare**” and “**findhelp®**” and “**findhelp.org**”).

1. **Overview.** SchoolCare is a health services and care coordination platform for Customers, their employees and agents, and the parents/legal guardians of Customer’s students (“**End Users**”).
2. **Term.** This Agreement will become effective on the last signature date of the Parties (the “**Effective Date**”). The initial term (“**Initial Term**”) of this Agreement will begin on the Effective Date and will continue for three years following the effective date, at which point this Agreement will automatically renew for a period of three years (“**Renewal Term**”), unless Customer provides 30 days’ notice to SchoolCare of its intention not to renew the Agreement. The Initial Term and any Renewal Terms are referred to, collectively, as the “**Term**.”
3. **Services.** Subject to the terms and conditions of this Agreement, SchoolCare grants Customer and its End Users a non-exclusive, non-transferable license to access and use SchoolCare’s hosted services (the “**Services**”), as described in Exhibit B (“**Scope of Services**”), which Scope of Services may be modified from time to time by mutual written agreement by the parties hereto (the “**Parties**”). To the extent any SchoolCare software is provided to Customer for installation on the Customer’s systems for use in connection with the Services, the SchoolCare software is included in the definition of Services and subject to the foregoing license. All software may only be used in support of Customer’s use of the Services and for no other purpose.
4. **Customer Responsibilities.** Customer shall designate Services and perform Customer’s responsibilities pursuant to the Scope of Services in Exhibit B. In order to be eligible for Services, Customer shall: (i) supply SchoolCare with sufficient information and data to reproduce any error or problem that is the subject of a support request; (ii) procure, install, operate and maintain computer hardware systems, operating system software, and other software, compatible with SchoolCare’s minimum requirements for the version of the Services to be supported; (iii) establish adequate operational backup provisions in the event of malfunctions or errors; (iv) maintain an operating environment free of any programming that might interfere with the functioning of the Services as supplied by SchoolCare; and (v) have installed the most current release of the relevant SchoolCare system or platform, or a



prior release still supported by SchoolCare, as well as any fixes made available to Customer by SchoolCare. Customer shall use all reasonable efforts to promptly promote and transition End Users to the Services.

5. Text Messaging Functionality. The Services may include access to functionality permitting Customer to message End Users (the “**Text Functionality**”). The Text Functionality is provided by a third party vendor and is not deemed part of the Services under this Agreement. Customer understands and agrees Text Functionality is provided by SchoolCare as-is, without warranties of any kind, and should not be used nor relied upon for communicating information relating to emergent medical conditions or medical emergencies. No Protected Health Information should be transmitted using the Text Functionality. To the extent permitted under SchoolCare’s agreement with the third party vendor of the Text Functionality, SchoolCare will pass through to Customer any warranties and other protections offered by the third party vendor. Customer is responsible for obtaining all necessary consents and permissions from End Users and ensuring those consents and permissions and the content of all messages comply with all applicable laws and regulations, including, but not limited to, the Telemarketing Consumer Protection Act. Customer shall indemnify, defend, and hold harmless SchoolCare and the third party vendor of the Text Functionality from and against any claims, liabilities, damages, costs, sanctions, or fines arising from (i) Customer’s breach of this Section and (ii) the content of any End User Messages.

6. Restrictions. Customer and its End Users may only use the Services as described in this Agreement, the SchoolCare Terms of Use, the SchoolCare Privacy Policy, and the SchoolCare End User License Agreement, which may be viewed at <https://SchoolCare.com/end-user-license-agreement-districts/> (the “**Documentation**”). Customer is responsible for ensuring its End Users comply with all relevant terms of this Agreement and any failure to comply will constitute a breach by Customer. Except as expressly authorized by this Agreement, Customer will not, and will not allow any End User or other third party to, (i) permit any third party to access or use the Services other than an End User; (ii) decompile, disassemble, reverse engineer, or otherwise attempt to derive the trade secrets embodied in the Services, except to the extent expressly permitted by applicable law; (iii) use the Service, or allow the transfer, transmission, export, or re-export of the Service or portion thereof, in violation of any export control laws or regulations administered by the U.S. Commerce Department or any other government agency; or (iv) remove any copyright, trademark, proprietary rights, disclaimer, or warning notice included on or embedded in any part of the Documentation and Service, including any screen displays, etc., or any other products or materials provided by SchoolCare hereunder. Under



no circumstances will SchoolCare be liable or responsible for any use, or any results obtained by the use, of the Services in conjunction with any services, software, or hardware that are not provided by SchoolCare. All such non-conforming use will be at Customer's sole risk and liability. Customer is responsible for ensuring its contractors or agents comply with all relevant terms of this Agreement.

7. Availability. The hosted elements of the Services will be available for remote access 99.5% of the time each calendar month of the Term, excluding Excused Outages (as defined below) ("**Availability**"). SchoolCare will attempt to schedule any planned maintenance or upgrades at times when usage of the Services is typically low, and will attempt to communicate any outages associated with planned maintenance or upgrades to its customers in advance via email or through notifications within the Services. Downtime as a result of any causes beyond the control of SchoolCare or that are not reasonably foreseeable by SchoolCare, including, without limitation, any of the causes noted below, are excluded from the Availability calculations (collectively, "**Excused Outages**"):

- a. Customer environment issues affecting connectivity or interfering with the Services, including without limitation, Customer's telecommunications connection or any other Customer software or equipment, Customer's firewall software, hardware or security settings, Customer's configuration of anti-virus software or anti-spyware or malware software, or operator error of Customer;
- b. Any third party software, hardware, or telecommunication failures, including Internet slow-downs or failures;
- c. Force majeure events including, without limitation fire, flood, earthquake, elements of nature or acts of God; third party labor disruptions, acts of war, terrorism, riots, civil disorders, rebellions or revolutions; quarantines, embargoes and other similar governmental action; catastrophic or unusual internet delays, denial of services attacks, or other hacking activities; or any other similar cause beyond the reasonable control of SchoolCare;
- d. Issues related to third party domain name system (DNS) errors or failures; and
- e. Emergency maintenance of the Services, for which Customer may not receive advanced notice.

In the event SchoolCare fails to achieve the Availability requirement, SchoolCare will use commercially reasonable efforts to correct the interruption as promptly as practicable.



8. Privacy. SchoolCare maintains a Privacy Policy which may be viewed at <https://schoolcare.com/privacy-policy>. SchoolCare and Customer represent that they each comply with all data privacy laws applicable to the data collected and stored on SchoolCare.

9. Family Educational Rights and Privacy SchoolCare receives and handles personally identifiable information from education records as a “school official” under the United States Family Education Rights and Privacy Act, 20 U.S.C. 1232g, 34 CFR Part 99 (“FERPA”), for the purpose of delivering the Health Services as contemplated by this Agreement. Customer agrees that it has obtained any necessary written consents from parents of students under the age of eighteen (18) and students age eighteen (18) and older in order to upload student data to SchoolCare.

SchoolCare agrees that personally identifiable information obtained from student education records will be used solely for the purposes of performing Services under this Agreement, and will not be disclosed to third parties except as required to provide Services to Customer contemplated in this Agreement, or otherwise as expressly permitted by FERPA and other applicable laws, without signed and dated written consent of the parent/legal guardian of a student under the age of 18, or of the student age 18 and older.

It is Customer’s responsibility to respond to requests for education records received by SchoolCare from third parties.

10. Information Security. SchoolCare maintains and enforces commercially reasonable practices, including administrative, technical, and physical safeguards to reasonably protect the confidentiality, availability, and integrity of Customer and End User data in alignment with requirements of applicable laws and regulations, including the Health Insurance Portability and Accountability Act (HIPAA). This includes, but is not limited to, encryption of data in transit when submitted across the Internet, access controls, firewalls and user authentication protocols. The Internet, however, is not entirely secured, and SchoolCare will not be responsible for security incidents not reasonably within its control.

If required by applicable laws, SchoolCare will promptly report to Customer any unauthorized access to Customer Data and, in the event that further notification is required by law, will support Customer notification to its End Users.

11. Connectivity. Customer and End Users are solely responsible for all telecommunication or Internet connections required to access the Services, as well as all hardware and software at Customer’s site. In addition to other third party costs that may apply, Customer agrees to pay for all telecommunications costs, fees and services required for and dedicated to Customer’s access to the Services.



12. Proprietary Rights. Customer acknowledges and agrees that (i) all Services are protected by intellectual property rights, as applicable, of SchoolCare and its vendors/licensors and that Customer has no right to transfer or reproduce any Services or any software provided with the Services or prepare any derivative works with respect to, or disclose Confidential Information (as defined in Section 20 (Confidentiality)) pertaining to, any Services or any part of them and (ii) that SchoolCare owns all right, title, and interest in and to the Services, including any changes or modifications made to the Services performed in connection with this Agreement, together with all ideas, architecture, algorithms, models, processes, techniques, user interfaces, database design and architecture, and “know-how” embodying the Services. Under no circumstances will Customer be deemed to receive title to any portion of the Services, title to which at all times will vest exclusively in SchoolCare. This is not a “work made for hire” agreement, as that term is defined in Section 101 of Title 17 of the United States Code. Customer will preserve all Services from any liens, encumbrances, and claims of any individual or entity. Customer will not use any Confidential Information disclosed by SchoolCare to Customer in connection with this Agreement to contest the validity of any intellectual property rights of SchoolCare or its licensors. Any such use of SchoolCare’s Confidential Information will constitute a material, non-curable breach of this Agreement. You will preserve all Services from any liens, encumbrances, and claims of any individual or entity. You will not use any of our information or data to contest the validity of any of our intellectual property or our licensors. Any such use of our information and data will constitute a material, non-curable breach of this Agreement. Unless otherwise indicated, trademarks that appear in these Services are trademarks of SchoolCare or its affiliates. All other trademarks not owned by SchoolCare or its affiliates that appear in the Service are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by SchoolCare and its affiliates. You agree not to display, disparage, dilute, or taint our trademarks in such a way that would misrepresent the ownership of such marks. Any permitted use of our trademark by you shall be to the benefit of SchoolCare.

13. Customer Data. Customer grants SchoolCare a non-exclusive, world-wide, royalty-free license to use the documents, information, graphics, data, content, and other materials input by Customer into the Services (the “**Customer Data**”) solely for the purposes of executing the Services described in this Agreement. Customer will be responsible for obtaining all rights, permissions, and authorizations to provide the Customer Data to SchoolCare for use as specified under this Agreement. At Customer’s discretion and subject to Customer’s rights under FERPA, SchoolCare may import data from third parties to add to Customer’s data hosted by SchoolCare. Customer represents that it will obtain and maintain all necessary agreements with such third parties to authorize SchoolCare to do so on Customer’s behalf. Except for the license granted in



this Section, nothing contained in this Agreement will be construed as granting SchoolCare any right, title, or interest in the Customer Data.

14. Deidentified Data. Notwithstanding the limitations in Section 12, SchoolCare may create and retain aggregated, deidentified information from Customer Data, including Customer's student data to demonstrate the effectiveness of SchoolCare Services, including in SchoolCare marketing materials, to improve SchoolCare Services and to develop and improve other educational products. All data will be deidentified in accordance with the standards set forth in FERPA and HIPAA.

15. Feedback. Customer may provide suggestions, comments, or other feedback (collectively, "Feedback") to SchoolCare with respect to its products and services, including the Services. Feedback is voluntary. SchoolCare may use Feedback for any purpose without obligation of any kind. To the extent a license is required under Customer's intellectual property rights to make use of the Feedback, Customer grants SchoolCare an irrevocable, non-exclusive, perpetual, fully-paid-up, royalty-free license to use the Feedback in connection with SchoolCare's business, including the enhancement of the Services.

16. Support and Maintenance. During the Term, SchoolCare will provide Customer with reasonable telephone support during SchoolCare's then-current business hours. SchoolCare will provide Customer Service updates and bug fixes that SchoolCare in its sole discretion makes generally available to its other similarly situated licensees at no charge. New or different functionality may be purchased by Customer, in its discretion, at SchoolCare's then-current pricing. SchoolCare will use commercially reasonable efforts to correct reproducible failures of the Service to perform in substantial accordance with their then-current Documentation.

17. Warranties.

17.1 Customer Warranty. Customer represents and warrants that (a) it has full power, capacity, and authority to enter into this Agreement and to grant the license set forth in Section 12 (Customer Data); (b) any Customer Data provided by Customer to SchoolCare for use in connection with the Services does not and will not infringe the intellectual property, publicity, or privacy rights of any person and is not defamatory, obscene, or in violation of applicable foreign, federal, state and local laws, rules and regulations (including but not limited to applicable policies and laws related to spamming, privacy, and consumer protection) (collectively, "**Applicable Law**"); and (c) its use of the Services will be in compliance with all Applicable Law.

17.2 SchoolCare Warranty. During the Term, SchoolCare represents and warrants (i) the Services will substantially comply with the Documentation; (ii) it shall use commercially



reasonable efforts to screen the Services for viruses, Trojan horses, worms, and other similar intentionally harmful or destructive code; and (iii) it shall comply with Applicable Law in performing this Agreement. In the event of a breach of the warranty in Section 17.2(i), SchoolCare's sole and exclusive liability and Customer's sole and exclusive remedy will be to perform the defective Service again. In the event SchoolCare is unable through reasonable efforts to correct the defective Service within thirty (30) days from receipt of notice from Customer of the breach, Customer may elect to terminate this Agreement.

17.3 Disclaimer of Warranties. EXCEPT AS PROVIDED IN SECTION 17.2 (SchoolCare WARRANTY), THE SERVICES ARE PROVIDED "AS IS" AND "AS-AVAILABLE," WITH ALL FAULTS, AND WITHOUT WARRANTIES OF ANY KIND. SchoolCare AND ITS VENDORS AND LICENSORS DISCLAIM ALL OTHER WARRANTIES, EXPRESS AND IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET ENJOYMENT, QUALITY OF INFORMATION, AND TITLE/NON-INFRINGEMENT. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SchoolCare OR ITS AUTHORIZED REPRESENTATIVES WILL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF SchoolCare'S OBLIGATIONS HEREUNDER. THE SERVICES MAY BE USED TO ACCESS AND TRANSFER INFORMATION OVER THE INTERNET. CUSTOMER ACKNOWLEDGES AND AGREES THAT SchoolCare AND ITS VENDORS AND LICENSORS DO NOT OPERATE OR CONTROL THE INTERNET AND THAT: (I) VIRUSES, WORMS, TROJAN HORSES, OR OTHER UNDESIRABLE DATA OR SOFTWARE; OR (II) UNAUTHORIZED USERS (E.G., HACKERS) MAY ATTEMPT TO OBTAIN ACCESS TO AND DAMAGE CUSTOMER'S DATA, WEB-SITES, COMPUTERS, OR NETWORKS. SchoolCare WILL NOT BE RESPONSIBLE FOR SUCH ACTIVITIES. CUSTOMER IS RESPONSIBLE FOR PRESERVING AND MAKING ADEQUATE BACKUPS OF ITS DATA.

18. Third Party E-mail Communication Functionality. Customer may elect to use functionality in the Services to send one-way e-mail communications to parents of students (the "E-mail Functionality"). Customer understands and agrees that (i) it shall use the E-mail Functionality in compliance with all applicable laws and regulations; (ii) the E-mail Functionality is provided by a third party provider over whom SchoolCare has no control; (iii) the communications may be unsecure and that student personal information should not be included in such communications; (iv) communications are not encrypted; (v) all use of the E-mail Functionality is subject to Customer's agreement to be bound by the terms and conditions located at www.sendgrid.com/policies/tos and (vi) use of the functionality is at Customer's sole risk.

SchoolCare provides the E-mail Functionality as a convenience to Customer, without warranties of any kind. SchoolCare disclaims all warranties express or implied with regard to the E-mail Functionality. IN NO EVENT WILL SchoolCare OR THE LICENSORS OR SUPPLIERS OF



THE E-MAIL FUNCTIONALITY BE LIABLE TO CUSTOMER OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, PUNITIVE, EXEMPLARY, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE E-MAIL FUNCTIONALITY, EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES. CUSTOMER WAIVES ANY AND ALL CLAIMS, NOW KNOWN OR LATER DISCOVERED, THAT IT MAY HAVE AGAINST SchoolCare OR THE LICENSORS OR SUPPLIERS OF THE E-MAIL FUNCTIONALITY. CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH REGARD TO THE E-MAIL FUNCTIONALITY IS TO CEASE USE OF THOSE ELEMENTS.

19. Indemnification. Customer agrees to indemnify and defend SchoolCare and its agents, employees, representatives, licensors, affiliates, corporate parents and subsidiaries from and against any and all claims, losses, demands, causes of action and judgments (including attorneys' fees and court costs) of third parties (collectively, "Claims") arising from or concerning any breach or alleged breach of this Agreement by Customer and to reimburse SchoolCare on demand for any losses, costs or expenses it incurs as a result of any such Claims.

20. Confidentiality. Each party may disclose to the other certain non-public information or materials relating to a party's products, intellectual property, business, marketing programs and efforts, personally identifiable information of the party's personnel, End Users, students and customers, and other confidential information and trade secrets ("**Confidential Information**").

Confidential Information does not include information that: (a) is or becomes publicly available through no breach by the receiving party of this Agreement; (b) was previously known to the receiving party prior to the date of disclosure, as evidenced by contemporaneous written records; (c) was acquired from a third party without any breach of any obligation of confidentiality; (d) was independently developed by a party hereto without reference to Confidential Information of the other party; or (e) is required to be disclosed pursuant to a subpoena or other similar order of any court or government agency, provided, however, that the party receiving such subpoena or order shall, when legally permissible, promptly inform the other party in writing and provide a copy thereof, and shall only disclose that Confidential Information necessary to comply with such subpoena or order. Except as expressly provided herein, the receiving party will not use or disclose any Confidential Information of the disclosing party without the disclosing party's prior written consent, except disclosure to and subsequent uses by the receiving party's employees or consultants on a need-to-know basis, provided that such employees or consultants have executed written agreements restricting use or disclosure of such Confidential Information that are at least as restrictive as the receiving party's obligations under this Section. The receiving party agrees to use at least the same care and precaution in protecting such Confidential Information as the receiving party uses to protect the receiving party's own Confidential Information, and in no event less than reasonable care. Each party acknowledges that due to the unique nature of the other party's Confidential Information,



the disclosing party may not have an adequate remedy solely in money or damages in the event of any unauthorized use or disclosure of its Confidential Information. In addition to any other remedies that may be available in law, in equity or otherwise, the disclosing party shall be entitled to seek injunctive relief to prevent such unauthorized use or disclosure.

21. Limitation of Liability and Damages. NEITHER SchoolCare NOR ITS VENDORS AND LICENSORS WILL HAVE ANY LIABILITY TO CUSTOMER OR ANY THIRD PARTY FOR ANY LOSS OF PROFITS, SALES, TRADING LOSSES, BUSINESS, DATA, OR OTHER INCIDENTAL, CONSEQUENTIAL, OR SPECIAL LOSS OR DAMAGE, INCLUDING EXEMPLARY AND PUNITIVE, OF ANY KIND OR NATURE RESULTING FROM OR ARISING OUT OF THIS AGREEMENT, INCLUDING USE OF OR INABILITY TO USE THE SERVICES. THE TOTAL LIABILITY OF SchoolCare AND ITS VENDORS AND LICENSORS TO CUSTOMER OR ANY THIRD PARTY ARISING OUT OF THIS AGREEMENT OR USE OF THE SERVICES IN CONNECTION WITH ANY CLAIM OR TYPE OF DAMAGE (WHETHER IN CONTRACT OR TORT, INCLUDING NEGLIGENCE) WILL NOT EXCEED THE GREATER OF \$10,000 OR THE FEES, IF ANY, ACTUALLY PAID BY CUSTOMER IN THE THREE MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO THE LIABILITY AND PAID FOR SERVICES. THIS LIMITATION OF LIABILITY WILL APPLY EVEN IF THE EXPRESS WARRANTIES SET FORTH ABOVE FAIL IN THEIR ESSENTIAL PURPOSE.

22. Termination.

22.1 Termination. SchoolCare reserves the right at any time to discontinue, temporarily or permanently, the Service or any part thereof or terminate any user's access to the Service or any part thereof. We may also modify, delete or adapt the Service at any time without any notice or obligation to the user at SchoolCare's sole discretion. Your right to use and otherwise access the Service is automatically terminated if you violated the Terms of Use. You agree that SchoolCare will not be liable to you or any third party for any modification, suspension, or discontinuation of the Service, or any part thereof. Upon termination for any reason, you must cease all access to the Service. All provisions of the Terms of Use as to limitation and disclaimer of warranty, limitation of liability, SchoolCare's ownership rights and your representations and indemnities shall survive termination.

This Agreement will terminate (a) on the thirtieth (30th) day after either party gives the other written notice of a breach by the other of any material term or condition of this Agreement, unless the breach is cured before that day; or (b) upon written notice by either party, immediately, if (i) a receiver is appointed for the other party or its property; (ii) if the other party becomes insolvent or unable to pay its debts as they mature in the ordinary course of business or makes a general assignment for the benefit of its creditors; or (iii) if any proceedings (whether voluntary or involuntary) are commenced against the other party under any bankruptcy or similar law and such **proceedings** are not vacated or set aside



within sixty (60) days from the date of commencement thereof. The following provisions will survive termination or expiration of this Agreement: 11 (Proprietary Rights), 17.3 (Disclaimer of Warranties), (for claims accruing prior to termination), 20 (Confidentiality), 21 (Limitation of Liability and Damages), 22 (Termination), and 24 (General Provisions). At any time during the Term, Customer may request a copy of the Customer Data at no additional charge. Within 30 days of termination of the Agreement, or as otherwise required by law or requested by Customer with reasonable notice to SchoolCare, SchoolCare will securely delete and destroy all Customer data marked by Customer within SchoolCare as “Private.” SchoolCare may transfer a copy of all other Customer data related to Customer students to the respective SchoolCare account of each parent or legal guardian, or to the account of the student age 18 or older. If no such account is maintained, SchoolCare will securely delete and destroy the “education records.” . Notwithstanding the above, SchoolCare will retain aggregated, deidentified information as noted in Section 13.

22.2 Suspension of Services. Notwithstanding any other provision of this Agreement, SchoolCare may, in its sole discretion, suspend Customer’s access to the Services for any of the following reasons (a) to prevent damages or risk to, or degradation of, the Services; (b) to comply with any law, regulation, court order, or other governmental request; or (c) to otherwise protect SchoolCare from potential legal liability. SchoolCare will use reasonable efforts to provide Customer with notice prior to or promptly following any suspension of the Services. SchoolCare will promptly restore access to the Services as soon as the event giving rise to suspension has been resolved. This Section will not be construed as imposing any obligation or duty on SchoolCare to monitor use of the Services.

23. Assignment. Customer may not assign this Agreement without the written consent of SchoolCare. SchoolCare may assign this Agreement to a successor entity in the event of a merger, acquisition or sale of all or substantially all of its assets.

24. General Provisions. This Agreement will be construed, interpreted, and performed according to the federal laws of the United States of America and the laws of the State of Texas, without giving effect to any principles of conflicts of law. Any action at law or in equity arising out of or directly or indirectly relating to this Agreement may be instituted only in the Federal or state courts located in Austin, Texas. The parties consent and submit to the personal jurisdiction of those courts for the purposes of any action related to this Agreement, and to extra-territorial service of process. Regardless of any statute or law to the contrary, any claim or cause of action that Customer may have arising out of or related to this Agreement must be filed within one (1) year after the claim or cause of action arose. This Agreement constitutes the entire understanding and agreement between the parties with respect to the transactions contemplated in this Agreement and supersedes all prior or contemporaneous oral or written



communications with respect to the subject matter of this Agreement, all of which are merged in this Agreement. This Agreement may not be modified, amended or in any way altered except by an instrument in writing signed by authorized representatives of both parties. In the event any provision of this Agreement is found invalid or unenforceable pursuant to judicial decree, the remainder of this Agreement will remain valid and enforceable according to its terms. Any failure by either party to strictly enforce any provision of this Agreement will not operate as a waiver of that provision or any subsequent breach of that provision. This Agreement may be accepted in electronic form (e.g., by an electronic or other means of demonstrating assent) and Customer's acceptance will be deemed binding between the parties. Neither party will contest the validity or enforceability of this Agreement, including under any applicable statute of frauds, because it was accepted or signed in electronic form. Electronically maintained records when produced in hard copy form shall constitute business records and shall have the same validity as any other generally recognized business records. **IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT IN THE EVENT ANY REMEDY HEREUNDER IS DETERMINED TO HAVE FAILED IN ITS ESSENTIAL PURPOSE, ALL LIMITATIONS OF LIABILITY AND EXCLUSIONS OF DAMAGES WILL REMAIN IN EFFECT.**

(end of Exhibit A)

**Exhibit B SchoolCare Scope of Services**

SchoolCare Services: A developer of a medical record system for schools, school employees and parents/legal guardians of students that includes an electronic form for health information collection and storage, and an administrator tool to view and manage the status of the health information collection process, inclusive of the following:

- Coordination of health services between school nurses, parents and student's health insurance plan <https://schoolcare.com/parents/careCoordination>
- Online storage for designated health information of End Users, inclusive of nurse visits and medications dispensed;
- Means for physicians to transmit health records via agreed-upon electronic means for inclusion in End User account information;
- Digitized physician reports from physicals for access as part of the user account files in the SchoolCare Services;
- Accounts for End Users, subject to acceptance of SchoolCare privacy policy <https://schoolcare.com/privacy-policy> and terms of use <https://schoolcare.com/terms-of-use> ;
- Delivery of health data insights and reports to school districts, public health organizations and other healthcare agencies, developed by SchoolCare or its third party partners, derived from identified and de-identified Customer student data and developed, provided, however, that such partners may use the data only to develop and provide this part of the Services to Customer on behalf of SchoolCare
- Facilitation of healthcare coordination and health interventions developed by SchoolCare or its third party partners, and derived from identified and deidentified Customer student data, provided, however, that we have receive applicable consents from the Customer and parents, and that such partners may use the data only to develop and provide this part of the Services to Customer on behalf of SchoolCare.
- Delivery of deidentified student data to state public health agencies to facilitate a school or district Customer's required reporting and for state public health agency interventions;
- Import of records from third parties at Customer's discretion and subject to Customer's rights under FERPA, provided that Customer has obtained all applicable consents;
- Training materials to help Customer manage support questions from its End Users
- Customer will engage in outreach to parents/guardians to encourage use of the SchoolCare Care Coordination Program, located at: <https://schoolcare.com/parents/careCoordination>

(end of Exhibit B)



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

04/12/2023

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Embroker Insurance Services LLC 5214F Diamond Heights Blvd. Unit 1261 San Francisco CA 94131		CONTACT NAME: Matthew Miller PHONE (A/C No, Ext): (844)436-2765 E-MAIL ADDRESS: certificates@embroker.com FAX (A/C, No):	
INSURED Aunt Bertha, a Public Benefit Corporation 3616 Far West Blvd Suite 117-454 Austin TX 78731		INSURER(S) AFFORDING COVERAGE INSURER A: Twin City Fire Insurance Company INSURER B: Sentinel Insurance Company Limited INSURER C: Clear Blue Specialty Insurance Company INSURER D: Scottsdale Insurance Company INSURER E: INSURER F:	
		NAIC # 29459 11000 37745 41297	

COVERAGES**CERTIFICATE NUMBER:** 27768**REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:	Y		57SBABN2254	01/19/2023	01/19/2024	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 1,000,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMP/OP AGG \$ 2,000,000
	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO OWNED AUTOS ONLY <input checked="" type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS NON-OWNED AUTOS ONLY	Y		57SBABN2254	01/19/2023	01/19/2024	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$ 10000	Y		57SBABN2254	01/19/2023	01/19/2024	EACH OCCURRENCE \$ 5,000,000 AGGREGATE \$ 5,000,000
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below Y/N <input checked="" type="checkbox"/> N	N/A		57WBCIO9797	01/19/2023	01/19/2024	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
C	Tech E&O / Cyber Liability			AX01-2052-03	01/19/2023	01/19/2024	Aggregate 5,000,000
C	Commercial Crime			CR01-100474-231	01/19/2023	01/19/2024	Aggregate 1,000,000
D	Excess Tech E&O / Cyber Liability			EKS3463117	01/19/2023	01/19/2024	Aggregate 5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Board of Education of Jefferson County is included as Additional Insured on the General Liability as required by written contract.

CERTIFICATE HOLDERBoard of Education of Jefferson County
Attn: Insurance/Real Estate Dept.
3332 Newburg Road
Louisville

KY 40218

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

© 1988-2015 ACORD CORPORATION. All rights reserved.



ADDITIONAL REMARKS SCHEDULE

AGENCY Embroker Insurance Services LLC		NAMED INSURED Aunt Bertha, a Public Benefit Corporation
POLICY NUMBER		
CARRIER	NAIC CODE	EFFECTIVE DATE:

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,

FORM NUMBER: _____ FORM TITLE: _____