

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

Shutterfly Lifetouch, LLC., a corporation organized under the laws of Minnesota with its principal place of business located at 11000 Viking Drive, Eden Prairie, MN 55344 (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 22, 2026 (the “**Effective Date**”) and shall continue for three (3) years, terminating on July 21, 2029.
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 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 **Sam Bolstad, Principal Corporate Attorney** 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 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”**. Nothing in this Agreement will be construed to preclude Provider from retaining archival copies of any Confidential Data to meet its audit, legal or file retention policies so long as the confidentiality of the information is maintained pursuant to the terms hereof.

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. For the avoidance of doubt, this restriction does not apply to Provider providing parents of photographed students the opportunity to purchase student and class pictures and yearbooks.
9. **Liability.** Provider agrees to be responsible for and assumes all liability subject to any limitations of liability set forth in the Service Agreement, 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 7.
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: Jim Jury

Title: Interim Chief of Academic Officer

Address: 3332 Newburg Rd Louisville, KY 40218

Phone: 502-485-8206

Email: jim.jury@jefferson.kyschools.us

The designated representative for the Provider for this DPA is:

Name: Sam Bolstad Title: Principle Corporate Attorney

Address: 11000 Viking Drive, Eden Prairie, MN 55344

Phone: 800-736-4753 Email: legal@shuttefly.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. 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.

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.~~ Provider's employees and authorized agents may access the Board's school grounds as reasonably necessary to perform the Services (including Picture Day photography), subject to Board policies and any background-check or visitor-management requirements communicated to Provider in advance.

STANDARD JEFFERSON COUNTY PUBLIC SCHOOLS DATA PRIVACY AGREEMENT

Version Date: 5.11.22

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

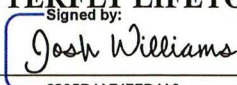
BOARD OF EDUCATION OF JEFFERSON COUNTY KENTUCKY

By: _____ Date: _____

Printed Name: Dr. H. Brian Yearwood

Title/Position: Superintendent

SHUTTERFLY LIFETOUGH, LLC

By:  Date: 7/20/2026
Signed by: 6205D4AF47FD4A0...

Printed Name: Josh Williams

Title/Position: Director, Host Field

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:

Shutterfly Lifetouch, LLC ("Lifetouch") is a trusted provider of school photography services throughout North America since 1936.

Scope of Data Privacy Agreement: As used in this DPA, Lifetouch is a "Provider" with respect to one or more of the following educational support services:

- Picture Day and other photography services.
- Lifetouch Portal - online service for the secure transfer of student data needed for Picture Day and provisioning of images to schools after Picture Day for the school's administrative needs.
- Picture Day Notify® -- email service providing school-to-parent notifications regarding Picture Day and the availability of pictures.
- Lifetouch Yearbooks -- collaborative yearbook building applications for K-8 and high schools respectively

In preparation for Picture Day, Lifetouch collects certain roster data from the school or district, to be used solely as follows:

- To produce and deliver to schools the products and services as described in the Photography Services Agreement (the "School Deliverables");
- To deliver Picture Day notices on behalf of the school and provide parents of students photographed opportunities to purchase student and class pictures and yearbooks;
- To verify parent authorization to order student photographs; and
- As otherwise specified by the Agreement.

For the avoidance of doubt, this DPA does not apply to (a) information collected from customers who opt to purchase products directly from Lifetouch and/or establish a Lifetouch family account; or (b) Lifetouch photographs, except as incorporated into the School Deliverables. In all cases, Lifetouch is and remains the copyright owner of its photographic images.

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 standard vendor pricing. Cumulative JCPS purchases und this agreement shall not exceed \$90,000 annually

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.	☒
	Other application technology meta data-Please specify:	
	School District Name	☒
Application Use Statistics	Meta data on user interaction with application	☒
Assessment	Standardized test scores	☐
	Observation data	☐
	Other assessment data-Please specify:	☐
Attendance	Student school (daily) attendance data	☐
	Student class attendance data	☐
Communications	Online communications captured (emails, blog entries)	☐
Conduct	Conduct or behavioral data	☐
Demographics	Date of Birth	☒
	Place of Birth	☐
	Gender	☒
	Ethnicity or race	☐
	Language information (native, or primary language spoken by student)	☐
	Other demographic information-Please specify:	☐
Enrollment	Student school enrollment	☒
	Student grade level	☒
	Homeroom	☒
	Guidance counselor	☐
	Specific curriculum programs	☐
	Year of graduation	☒

Category of Data	Elements	Check if Used by Your System
	Other enrollment information-Please specify:	☐
Parent/Guardian Contact Information	Address	☐
	Email	☒
	Phone	☐
Parent/Guardian ID	Parent ID number (created to link parents to students)	☐
Parent/Guardian Name	First and/or Last	☐
Schedule	Student scheduled courses	☐
	Teacher names	☒
Special Indicator	English language learner information	☐
	Low income status	☐
	Medical alerts/ health data	☐
	Student disability information	☐
	Specialized education services (IEP or 504)	☐
	Living situations (homeless/foster care)	☐
	Other indicator information-Please specify:	☐
Student Contact Information	Address	☒
	Email	☒
	Phone	☐
Student Identifiers	Local (School district) ID number	☒
	State ID number	☐
	Provider/App assigned student ID number	☐
	Student app username	☐
	Student app passwords	☐
Student Name	First and/or Last	☒
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	☐

Category of Data	Elements	Check if Used by Your System
Student Survey Responses	Student responses to surveys or questionnaires	☐
Student work	Student generated content; writing, pictures, etc.	☐
	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:	☐

Category of Data	Elements	Check if Used by Your System
Other	Please list each additional data element used, stored, or collected by your application:	☐
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable.	☐

EXHIBIT “C”

DEFINITIONS

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



CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
05/14/2026

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 Aon Risk Services Central, Inc. Minneapolis MN office 5600 West 83rd Street 8200 Tower, Suite 1100 Minneapolis MN 55437 USA	CONTACT NAME: PHONE (A/C. No. Ext): (866) 283-7122 FAX (A/C. No.): (800) 363-0105 E-MAIL ADDRESS:
INSURED Shutterfly LLC Shutterfly Lifetouch LLC 11000 Viking Drive Eden Prairie MN 55344 USA	INSURER(S) AFFORDING COVERAGE INSURER A: Zurich American Ins Co INSURER B: American Guarantee & Liability Ins Co INSURER C: AIG Specialty Insurance Company INSURER D: INSURER E: INSURER F:

Holder Identifier : 265485

COVERAGES CERTIFICATE NUMBER: 570119960017 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.

Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDITIONAL INSURED	SUBROGATION	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	☒ COMMERCIAL GENERAL LIABILITY ☐ CLAIMS-MADE ☒ OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: ☒ POLICY ☐ PROJECT ☐ LOC OTHER:			GLO104083810	06/30/2025	06/30/2026	EACH OCCURRENCE \$2,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$500,000 MED EXP (Any one person) \$5,000 PERSONAL & ADV INJURY \$2,000,000 GENERAL AGGREGATE \$4,000,000 PRODUCTS - COM/OP AGG \$4,000,000
A	☒ AUTOMOBILE LIABILITY ☒ ANY AUTO ☐ OWNED AUTOS ONLY ☐ HIRED AUTOS ONLY ☒ Comp/Collision 1,000 D ☐ SCHEDULED AUTOS ☐ NON-OWNED AUTOS ONLY			BAP 1040839 10	06/30/2025	06/30/2026	COMBINED SINGLE LIMIT (Ea accident) \$2,000,000 BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)
B	☒ UMBRELLA LIAB ☐ EXCESS LIAB ☐ DED ☐ RETENTION ☒ OCCUR ☐ CLAIMS-MADE			AUC138447901	06/30/2025	06/30/2026	EACH OCCURRENCE \$10,000,000 AGGREGATE \$10,000,000 Products/Completed O \$10,000,000
A	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 N	N/A	WC104083610 WC104083710	06/30/2025 06/30/2025	06/30/2026 06/30/2026	☒ PER STATUTE ☐ OTHER E.L. EACH ACCIDENT \$1,000,000 E.L. DISEASE-EA EMPLOYEE \$1,000,000 E.L. DISEASE-POLICY LIMIT \$1,000,000
c	Cyber Liability			021429276 SIR applies per policy terms & conditions	09/29/2025	09/29/2026	Limit \$10,000,000

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

RE: LID Number (Parent LID for School District): 265485, Territory Code: HM. Jefferson County Board of Education is included as Additional Insured in accordance with the policy provisions of the General Liability policy.

CERTIFICATE HOLDER

CANCELLATION

Board of Education of Jefferson County Attn: Insurance/Real Estate Dept. 3332 Newburg Road Louisville KY 40218 USA	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 <i>Aon Risk Services Central, Inc.</i>
---	---

Certificate No : 570119960017



Service Agreement

Jefferson County School District

Lifetouch ID: 265485
Account Representative Email:
alexis.heeke@lifetouch.com

School Year(s): 2026-2027
Agreement Length: 1

Account Information

Jefferson County School District
3332 Newburg Rd
Louisville, KY 40218

Main Phone: 502-485-3011
Enrollment: 97600
Grades: Pre-K - 12

Summary of Programs Provided

Fall Individuals

Account Services

- ☐ Yearbook - Media CD/DMD
- ☐ Storefront
- ☒ Lifetouch Portal

Storefront Contact:

Lifetouch Portal Contact: Jesse Harris

Picture Day Notify is a complimentary service included when parent/guardian emails are provided.

Contact information

Contact Name	Title	Phone	Email
Alicia Waskom		502-485-3011	alicia.waskom@jefferson.kyschools.us

Agreement Terms

AUTHORIZED ACTIVITY: The account noted above (referred to as "you") designates Shutterfly Lifetouch, LLC (referred to as "Lifetouch") as your professional photographer and authorizes Lifetouch to: (i) photograph all students and staff who participate in "Picture Day" or other photography events, and (ii) produce and deliver photographs and services for the programs identified above. If the account is designated as exclusive, you agree not to use any third party for the programs identified above. These terms & conditions shall be considered the "Agreement". **ACCOUNT DATA:** You are solely responsible for obtaining staff and parent or guardian consent to or opt out of: (i) participation in all events and activities, and (ii) inclusion in class photographs or yearbooks (if included in services). You will provide us with access to students and staff, and use of your facilities, property, and information for the purpose of performing the services, including Picture Day or event administration, fulfillment and distribution of photographs and yearbooks to you, delivery of Picture Day or event notices, and providing parents or guardians of photographed students opportunities to purchase individual and class pictures and yearbooks (if included in services). **PAYMENT OBLIGATION:** You agree to promptly pay all invoices or monies owed by you to Lifetouch and in no case later than thirty (30) days. Any invoices that remain unpaid after sixty (60) days shall accrue interest at a rate of one (1) percent per month or the maximum amount allowed under applicable law and may accumulate fees for collection services. Lifetouch may remove your access to value-added goods and services, such as the Lifetouch Portal, until invoices are paid in full. Lifetouch provides access to value-added goods and services as a courtesy to customers; termination of this Agreement or failure to renew will result in removal of your ongoing access to these goods and services, including the Lifetouch Portal. **DATA PRIVACY:** Lifetouch will not disclose confidential information provided by you or use or retain it for any purpose other than performing the services or other internal uses as allowed by law. Lifetouch agrees to comply with laws, regulations and governmental orders governing the privacy and security of personal information including, where applicable and without limitation, the Family Educational Rights in Privacy Act. **COPYRIGHT:** Lifetouch is and remains the copyright owner of all photographic images created in connection with this agreement. If Lifetouch is obligated to provide photographic images to you as part of the services provided under this agreement, Lifetouch hereby grants you a nonexclusive, irrevocable, royalty-free license to use such photographic images solely for your administrative and educational purposes. **CANCELLATION:** Within any term, this Agreement may only be terminated i) by the written agreement of both parties, or ii) for convenience only more than ninety (90) days prior to the first photography event of that term. If you terminate this Agreement under the preceding sentence or reduce the number, kind, or amount of services and received anything of value from Lifetouch as part of this Agreement, you agree to immediately repay Lifetouch for the full value of any products or services received. In order to cancel this Agreement or modify the services under this paragraph, contact your Lifetouch account representative in writing. **MODIFICATION or ASSIGNMENT:** Lifetouch may modify the terms of this agreement or terminate this agreement upon notice to you. You may terminate this agreement if Lifetouch notifies you of a material change. If you do not terminate this agreement within 30 days after you receive notice of a change to the terms, you will be deemed to have accepted the change. Lifetouch's liability for any breach is limited to the amount you paid for services. Neither party is liable for delays or losses as a result of strikes, accidents, government restrictions, acts of God, acts of war, or other causes beyond its control, and such delays will not constitute a breach of contract. Lifetouch's liability for any breach is limited to the amount you paid for services. Lifetouch may assign, transfer, or delegate its rights or obligations under this Agreement, in whole or in part, without consent to its affiliates or to a successor-in-interest in connection with a merger, acquisition, corporate reorganization, or a sale of all or substantially all of Lifetouch's assets. **INSURANCE:** During the term of the agreement, Lifetouch agrees to maintain, at Lifetouch's expense, insurance coverage of the types and limits reflected on the attached certification of insurance in full force and effect with a company that has an A.M. Best rating of not less than A-. Commercial general liability insurance shall include you as additional insured and require thirty (30) days' notice of cancellation. Further, Lifetouch's insurance will be primary, and any insurance maintained by you shall be excess and non-contributory. Lifetouch agrees to waive and shall require its insurer to waive its right of subrogation in your favor solely with respect to workers' compensation insurance. **QUALIFIED, TRAINED, CERTIFICATED, AND LICENSED PERSONNEL:** Lifetouch shall provide services under this Agreement by appropriately trained and qualified staff. Lifetouch shall be responsible for verifying qualifications, providing training, and monitoring all staff certification at its own expense.

Signatures

Lexi Wolfe

Sales Account Executive - School

Alicia Waskom