

Version 2.0 Agreement Approved: June 2019

**DATA PRIVACY AGREEMENT (DPA)
FOR TEXAS K-12 INSTITUTIONS**

Lewisville Independent School District

and

Shutterfly Lifetouch, LLC

Background and Instructions

History of Agreement- This agreement has been drafted by the Texas Student Privacy Alliance (TXSPA). The Alliance is a collaborative group of Texas school districts that share common concerns around student and data privacy. The Texas K-12 CTO Council is the organization that sponsors the TXSPA and the TXSPA is the Texas affiliate of the national Student Data Privacy Consortium (SDPC). The SDPC works with otherstate alliances by helping establish common data privacy agreements unique to the jurisdiction of each state. This Texas agreement was drafted specifically for K-12 education institutions and included broad stakeholder input from Texas school districts, statewide associations such as TASB, TASA, and TASBO, and the Texas Education Agency. The purpose of this agreement is to set standards of both practice and expectations around data privacy such that all parties involved have a common understanding of expectations. This agreement also provides a mechanism (Exhibit E- General Offer of Terms) that would allow an Operator to extend the ability of other Texas school districts to be covered under the terms of the agreement should an Operator sign Exhibit E. This mechanism is intended to create efficiencies for both Operators and LEAs and generally enhance privacy practices and expectations for K-12 institutions and for companies providing services to K-12 institutions.

Instructions for Operators: This agreement is intended to be provided to an Operator from a LEA. The Operator should fully read the agreement and is requested to complete the below areas of the agreement. Once the Operator accepts the terms of the agreement, the Operator should wet sign the agreement and return it to the LEA. Once the LEA signs the agreement, the LEA should provide a signed copy of the agreement to the Operator.

Article/Exhibit	Box #	Description
Cover Page	Box # 3	Official Name of Operator
Cover Page	Box # 4	Date Signed by Operator
Recitals	Box #5	Contract Title for Service Agreement
Recitals	Box #6	Date of Service Agreement
Article 7	Boxes #7-10	Operator's designated representative
Signature Page	Boxes #15-19	Authorized Operator's representative signature
Exhibit A	Box #25	Description of services provided
Exhibit B	All Applicable Boxes	<ul style="list-style-type: none"> • Operator notates if data is collected to provide the described services. • Defines the schedule of data required for the Operator to provide the services outlined in Exhibit A
Exhibit D	All Applicable Boxes	(Optional Exhibit): Defines deletion or return of data expectations by LEA

Exhibit E	All Applicable Boxes	(Optional Exhibit): Operator may, by signing the Form of General Offer of Privacy Terms (General Offer, attached as <u>Exhibit E</u>), be bound by the terms of this DPA to any other Subscribing LEA who signs the acceptance in said Exhibit.
Exhibit F	Boxes # 25-29	A list of all Subprocessors used by the Operator to perform functions pursuant to the Service Agreement, list security programs and measures, list Operator's security measures

Instructions for LEA and/or Subscribing LEA: This agreement is intended to be provided to an Operator from a LEA. Upon receiving an executed agreement from an Operator, the LEA should fully review the agreement and if agreeable, should have an authorized LEA contact wet sign the agreement. Once signed by both the Operator and LEA, the LEA should send a copy of the signed agreement to the Operator.

Article/Exhibit	Box #	Description
Cover Page	Box # 1	Official Name of LEA
Cover Page	Box #2	Date Signed by LEA
Article 7	Boxes #11-14	LEA's designated representative
Signature Page	Boxes #20-24	Authorized LEA representative's signature
Exhibit D	All Applicable Boxes	(Optional Exhibit): Defines deletion or return of data expectations by LEA
Exhibit E	All Applicable Boxes	(Optional Exhibit) Only to be completed by a Subscribing LEA

RECITALS

WHEREAS, the Operator has agreed to provide the Local Education Agency (“LEA”) with certain digital educational services (“Services”) according to contracts titled “Service Agreements” [Box 5] and dated 2021-2022 school year (the “Service Agreement”), and

WHEREAS, in order to provide the Services described in the Service Agreement, the Operator may receive or create and the LEA may provide documents or data that are covered by federal statutes, among them, the Federal Educational Rights and Privacy Act (“FERPA”) at 20 U.S.C. 1232g (34 CFR Part 99), Children’s Online Privacy Protection Act (“COPPA”), 15 U.S.C. 6501-6506, and Protection of Pupil Rights Amendment (“PPRA”) 20 U.S.C. 1232h; and

WHEREAS, the documents and data transferred from LEAs and created by the Operator’s Services are also subject to state student privacy laws, including Texas Education Code Chapter 32; and

WHEREAS, the Operator may, by signing the "General Offer of Privacy Terms", agree to allow other LEAs in Texas the opportunity to accept and enjoy the benefits of this DPA for the Services described within, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Nature of Services Provided.** The Operator has agreed to provide digital educational services as outlined in Exhibit A and the Agreement.
2. **Purpose of DPA.** For Operator to provide services to the LEA it may become necessary for the LEA to share certain LEA Data. This DPA describes the Parties’ responsibilities to protect Data.
3. **Data to Be Provided.** In order for the Operator to perform the Services described in the Service Agreement, LEA shall provide the categories of data described in the Schedule of Data, attached as Exhibit B.
4. **DPA Definitions.** The definitions of terms used in this DPA are found in Exhibit C. In the event of a conflict, definitions used in this DPA shall prevail over terms used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Ownership of Data.** All Data transmitted to the Operator pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Operator further acknowledges and agrees that all copies of such Data transmitted to the Operator, 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 Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Data contemplated per the Service Agreement shall remain the exclusive property of the LEA.
2. **Operator Materials.** Operator retains all right, title and interest in and to any and all of Operator's software, materials, tools, forms, documentation, training and implementation materials and intellectual property ("Operator Materials"). Operator grants to the LEA a personal, nonexclusive license to use the Operator Materials for its own non-commercial, incidental use as set forth in the Service Agreement. Operator represents that it has all intellectual property rights necessary to enter into and perform its obligations in this DPA and the Service Agreement, warrants to the District that the District will have use of any intellectual property contemplated by the Service Agreement free and clear of claims of any nature by any third Party including, without limitation, copyright or patent infringement claims, and agrees to indemnify the District for any related claims.
3. **Parent Access.** LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Data on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Operator shall respond in a reasonably timely manner (and no later than 28 days from the date of the request) to the LEA's request for Data in a pupil's records held by the Operator to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Operator to review any of the Data accessed pursuant to the Services, the Operator shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.
4. **Data Portability.** Operator shall, at the request of the LEA, make Data available including Pupil Generated Content in a readily accessible format.
5. **Third Party Request.** Should a Third Party, including law enforcement or a government entity, contact Operator with a request for data held by the Operator pursuant to the Services, the Operator shall immediately (within 1 business day), and to the extent legally permitted, redirect the Third Party to request the data directly from the LEA, notify the LEA of the request, and provide a copy of the request to the LEA. Furthermore, if legally permissible, Operator shall promptly notify the LEA of a subpoena compelling disclosure to a Third Party and provide a copy of the subpoena with sufficient time for the LEA to raise objections to the subpoena. The Operator will not use, disclose, compile, transfer, or sell the Data and/or any portion thereof to any third party or other entity or allow any other third party or other entity to use, disclose, compile, transfer or sell the Data and/or any portion thereof. Notwithstanding any provision of this DPA or Service Agreement to the contrary, Operator understands that the LEA is subject to and will comply with the Texas Public Information Act (Chapter 552, Texas Government Code). Operator understands and agrees that information, documentation and other material in connection with the DPA and Service Agreement may be subject to public disclosure.
6. **No Unauthorized Use.** Operator shall use Data only for the purpose of fulfilling its duties and obligations under the Service Agreement and will not share Data with or disclose it to any Third Party without the prior written consent of the LEA, except as required by law or to fulfill its duties and obligations under the Service Agreement.
7. **Subprocessors.** All Subprocessors used by the Operator to perform functions pursuant to the Service Agreement shall be identified in Exhibit F. Operator shall either (1) enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, such that the Subprocessors agree to protect Data in a manner the same as or better than as provided pursuant to the terms of this DPA, or (2) indemnify and hold harmless the LEA, its officers, agents, and employees from any and all claims, losses, suits, or liability including attorneys' fees for damages or costs resulting from the acts or omissions of its Subprocessors. Operator shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this DPA. Subprocessors shall agree to the provisions of the DPA regarding governing law, venue, and jurisdiction.

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With State and Federal Law.** LEA shall provide data for the purposes of the Service Agreement in compliance with FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA as these laws and regulations apply to the contracted services. The LEA shall not be required to provide Data in violation of applicable laws. Operator may not require LEA or users to waive rights under applicable laws in connection with use of the Services.
2. **Consider Operator as School Official.** The Parties agree that Operator is a “school official” under FERPA and has a legitimate educational interest in personally identifiable information from education records. For purposes of the Service Agreement and this DPA, Operator: (1) provides a service or function for which the LEA would otherwise use employees; (2) is under the direct control of the LEA with respect to the use and maintenance of education records; and (3) is subject to the requirements of FERPA governing the use and redisclosure of personally identifiable information from education records
3. **Reasonable Precautions.** LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.
4. **Unauthorized Access Notification.** LEA shall notify Operator promptly of any known unauthorized access. LEA will assist Operator in any efforts by Operator to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF OPERATOR

1. **Privacy Compliance.** Operator may receive Personally Identifiable Information (“PII”) from the District in the course of fulfilling its duties and obligations under the Service Agreement. The Operator shall comply with all applicable State and Federal laws and regulations pertaining to data privacy and security including FERPA, COPPA, PPRA, Texas Education Code Chapter 32, and all other Texas privacy statutes cited in this DPA.
2. **Employee Obligation.** Operator shall require all employees and agents who have access to Data to comply with all applicable provisions of this DPA with respect to the data shared under the Service Agreement. Operator agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Data pursuant to the Service Agreement.
3. **De-identified Information.** De-identified Information may be used by the Operator only for the purposes of development, product improvement, to demonstrate or market product effectiveness, or research as any other member of the public or party would be able to use de-identified data pursuant to 34 CFR 99.31(b). Operator agrees not to attempt to re-identify De-identified Information and not to transfer De-identified Information to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to LEA who has provided prior written consent for such transfer. Operator shall not copy, reproduce or transmit any De-identified Information or other Data obtained under the Service Agreement except as necessary to fulfill the Service Agreement.
4. **Access To, Return, and Disposition of Data.** Upon written request of LEA, Operator shall dispose of or delete all Data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained, and transfer said data to LEA or LEA’s designee within sixty (60) days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Operator acknowledges LEA’s obligations regarding retention of governmental data, and shall not destroy Data except as permitted by LEA. Nothing in the Service Agreement shall authorize Operator to maintain Data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Data; (2) Data Destruction; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Operator shall provide written notification to LEA when the Data has been disposed of.

The duty to dispose of Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA. The LEA may employ a "Request for Return or Deletion of Data" FORM, a sample of this form is attached on Exhibit "D"). Upon receipt of a request from the LEA, the Operator will immediately provide the LEA with any specified portion of the Data within five (5) business days of receipt of said request.

5. **Targeted Advertising Prohibition.** Operator is prohibited from using or selling Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Operator; (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to LEA; or (d) use the Data for the development of commercial products or services, other than as necessary to provide the Service to LEA. This section does not prohibit Operator from generating legitimate personalized learning recommendations.
6. **Access to Data.** Operator shall make Data in the possession of the Operator available to the LEA within five (5) business days of a request by the LEA.

ARTICLE V: DATA PROVISIONS

1. **Data Security.** The Operator agrees to abide by and maintain adequate data security measures, consistent with industry standards and technology best practices, to protect Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Operator are set forth below. Operator shall further detail its security programs and measures in Exhibit F. These measures shall include, but are not limited to:
 - a. **Passwords and Employee Access.** Operator shall secure usernames, passwords, and any other means of gaining access to the Services or to Data, at a level consistent with an industry standard agreed upon by LEA (e.g. suggested by Article 4.3 of NIST 800-63-3). Operator shall only provide access to Data to employees or subprocessors that are performing the Services. Employees with access to Data shall have signed confidentiality agreements regarding said Data. All employees with access to Data shall pass criminal background checks.
 - b. **Security Protocols.** Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Operator shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment.
 - c. **Employee Training.** The Operator shall provide periodic security training to those of its employees who operate or have access to the system.
 - d. **Security Technology.** When the Services are accessed using a supported web browser, Secure Socket Layer ("SSL") or equivalent technology shall be employed to protect data from unauthorized access. The service security measures shall include server authentication and data encryption. Operator shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.
 - e. **Security Contact.** Operator shall provide the name and contact information of Operator's Security Contact on Exhibit F. The LEA may direct security concerns or questions to the Security Contact.
 - f. **Periodic Risk Assessment.** Operator shall conduct periodic risk assessments and remediate any identified security and privacy vulnerabilities in a timely manner. Upon request, Operator will provide the LEA an executive summary of the risk assessment or equivalent report and confirmation of remediation.

- g. Backups.** Operator agrees to maintain backup copies, backed up at least daily, of Data in case of Operator's system failure or any other unforeseen event resulting in loss of any portion of Data.
 - h. Audits.** Within 30 days of receiving a request from the LEA, and not to exceed one request per year, the LEA may audit the measures outlined in the DPA. The Operator will cooperate fully with the LEA and any local, state, or federal agency with oversight authority/jurisdiction in connection with any audit or investigation of the Operator and/or delivery of Services to students and/or LEA, and shall provide full access to the Operator's facilities, staff, agents and LEA's Data and all records pertaining to the Operator, LEA and delivery of Services to the Operator. Failure to cooperate shall be deemed a material breach of the DPA. The LEA may request an additional audit if a material concern is identified.
 - i. Incident Response.** Operator shall 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 any portion of Data, including PII, and agrees to provide LEA, upon request, an executive summary of the written incident response plan.
- 2. Data Breach.** When Operator reasonably suspects and/or becomes aware of an unauthorized disclosure or security breach concerning any Data covered by this Agreement, Operator shall notify the District within 24 hours. The Operator shall take immediate steps to limit and mitigate the damage of such security breach to the greatest extent possible. If the incident involves criminal intent, then the Operator will follow direction from the Law Enforcement Agencies involved in the case.
- a.** The security breach notification to the LEA shall be written in plain language, and address the following

 - 1. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
 - 2. A description of the circumstances surrounding the disclosure or breach, including the actual or estimated, time and date of the breach, and Whether the notification was delayed as a result of a law enforcement investigation.
 - b.** Operator agrees to adhere to all requirements in applicable state and federal law with respect to a Data breach or disclosure, including any required responsibilities and procedures for notification or mitigation
 - c.** In the event of a breach or unauthorized disclosure, the Operator shall cooperate fully with the LEA, including, but not limited to providing appropriate notification to individuals impacted by the breach or disclosure. Operator will reimburse the LEA in full for all costs incurred by the LEA in investigation and remediation of any Security Breach caused in whole or in part by Operator or Operator's subprocessors, including but not limited to costs of providing notification and providing one year's credit monitoring to affected individuals if PII exposed during the breach could be used to commit financial identity theft.
 - d.** The LEA may immediately terminate the Service Agreement if the LEA determines the Operator has breached a material term of this DPA.
 - e.** The Operator's obligations under Section 7 shall survive termination of this DPA and Service Agreement until all Data has been returned and/or Securely Destroyed.

ARTICLE VI- GENERAL OFFER OF PRIVACYTERMS

- 1. **General Offer of Privacy Terms.** Operator may, by signing the attached Form of General Offer of Privacy Terms (General Offer, attached as Exhibit E), be bound by the terms of this DPA to any other LEA who signs the acceptance in said Exhibit.

ARTICLE VII: MISCELLANEOUS

- 1. **Term.** The Operator shall be bound by this DPA for the duration of the Service Agreement or so long as the Operator maintains any Data. Notwithstanding the foregoing, Operator agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.
- 2. **Termination.** In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.
- 3. **Effect of Termination Survival.** If the Service Agreement is terminated, the Operator shall dispose of all of LEA’s Data pursuant to Article IV, section 5.
- 4. **Priority of Agreements.** This DPA shall govern the treatment of Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes cited in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, terms of service, privacy policy, or other writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph, all other provisions of the Service Agreement shall remain in effect.
- 5. **Notice.** All notices or other communication required or permitted to be given hereunder must be in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first-class mail, postage prepaid, sent to the designated representatives before: The designated representative for the Operator for this Agreement is:

First Name: Laurie [Box 7]
 Last Name: Dechery [Box 8]
 Operator’s Company Name: Shutterfly Lifetouch, LLC [Box 9]
 Title of Representative: Associate General Counsel [Box 10]

The designated representative for the LEA for this Agreement is:

First Name: CRAIG [Box 11]
 Last Name: MARTIN [Box 12]
 LEA’s Name: LEWISVILLE ISD [Box 13]
 Title of Representative: EXEC. DIRECTOR OF PROCUREMENT AND CONTRACTS [Box 14]

6. **Entire Agreement.** This DPA constitutes the entire agreement of the parties relating to the subject matter and supersedes all prior communications, representations, or agreements, oral or written, by the Parties. 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.
7. **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.
8. **Governing Law: Venue and Jurisdiction.** THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF TEXAS, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY IN WHICH THIS AGREEMENT IS FORMED FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.
9. **Authority.** Operator represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Data and/or any portion thereof, or may own, lease or control equipment or facilities of any kind where the Data and portion thereof is stored, maintained or used in any way.
10. **Waiver.** Waiver by any party to this DPA of any breach of any provision of this DPA or warranty of representation set forth herein shall not be construed as a waiver of any subsequent breach of the same or any other provision. The failure to exercise any right under this DPA shall not operate as a waiver of such right. All rights and remedies provided for in this DPA are cumulative. Nothing in this DPA shall be construed as a waiver or relinquishment of any governmental immunities or defenses on behalf of the LEA, its trustees, officers, employees, and agents as a result of the execution of this DPA or performance of the functions or obligations described herein.
11. **Assignment.** The Parties may not assign their rights, duties, or obligations under this DPA, either in whole or in part, without the prior written consent of the other Party except that either party may assign any of its rights and obligations under this DPA without consent in connection with any merger (including without limitation by operation of law), consolidation, reorganization, or sale of all or substantially all of its related assets or similar transaction. This DPA inures to the benefit of and shall be binding on the Parties' permitted assignees, transferees and successors.

[Signature Page Follows]

IN WITNESS WHEREOF, the parties have executed this DATA PRIVACY AGREEMENT FOR TEXAS K-12 INSTITUTIONS as of the last day noted below.

Operator's Representative:

BY:  [Box 15] Date: 11/13/2021 [Box 16]
DocuSigned by: E4D02B8212614CC...

Printed Name: Andy Panos [Box 17] Title/Position: Vice President Sales [Box 18]

Address for Notice Purposes: 11000 Viking Drive, Eden Prairie, MN 55344 [Box 19]

LEA's Representative:

BY:  [Box 20] Date: 12/1/2021 [Box 21]

Printed Name: CRAIG MARTIN [Box 22] Title/Position: EXEC. DIRECTOR OF PROCUREMENT AND CONTRACTS [Box 23]

Address for Notice Purposes: PO Box 217, LEWISVILLE, TX 75067 [Box 24]

Note: Electronic signature not permitted.

EXHIBIT "A"

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

Scope of DPA: As used in this DPA, Lifetouch is a "Provider" with respect to one or more of the following online educational support 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.
- **Parent Notify®** -- email service providing school-to-parent Picture Day notifications
- **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 (see Exhibit B), 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 DPA.

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.

EXHIBIT “ B”

SCHEDULE OF DATA

Instructions: Operator should identify if LEA data is collected to provide the described services. If LEA data is collected to provide the described services, check the boxes indicating the data type collected. If there is data collected that is not listed, use the “Other” category to list the data collected.

- We do not collect LEA Data to provide the described services.
- We do collect LEA Data to provide the described services.

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.	<input type="checkbox"/>
	Other application technology meta data-Please specify:	<input type="checkbox"/>
Application Use Statistics	Meta data on user interaction with application- Please specify:	<input type="checkbox"/>
Assessment	Standardized test scores	<input type="checkbox"/>
	Observation data	<input type="checkbox"/>
	Other assessment data-Please specify:	<input type="checkbox"/>
Attendance	Student school (daily) attendance data	<input type="checkbox"/>
	Student class attendance data	<input type="checkbox"/>
Communications	Online communications that are captured (emails, blog entries)	<input type="checkbox"/>
Conduct	Conduct or behavioral data	<input type="checkbox"/>
	Date of Birth	<input type="checkbox"/>

Demographics	Place of Birth	<input type="checkbox"/>
	Gender	<input type="checkbox"/>
	Ethnicity or race	<input type="checkbox"/>
	Language information (native, preferred or primary language spoken by student)	<input type="checkbox"/>
	Other demographic information-Please specify:	<input type="checkbox"/>
Enrollment	Student school enrollment	<input checked="" type="checkbox"/>
	Student grade level	<input checked="" type="checkbox"/>
	Homeroom	<input checked="" type="checkbox"/>
	Guidance counselor	<input type="checkbox"/>
	Specific curriculum programs	<input type="checkbox"/>
	Year of graduation	<input type="checkbox"/>
	Other enrollment information-Please specify:	<input type="checkbox"/>
Parent/Guardian Contact Information	Address	<input type="checkbox"/>
	Email	<input checked="" type="checkbox"/>
	Phone	<input type="checkbox"/>
Parent/Guardian ID	Parent ID number (created to link parents to students)	<input type="checkbox"/>
Parent/Guardian Name	First and/or Last	<input type="checkbox"/>
Schedule	Student scheduled courses	<input type="checkbox"/>
	Teacher names	<input type="checkbox"/>
Special Indicator	English language learner information	<input type="checkbox"/>
	Low income status	<input type="checkbox"/>
	Medical alerts /health data	<input type="checkbox"/>
	Student disability information	<input type="checkbox"/>
	Specialized education services (IEP or 504)	<input type="checkbox"/>
	Living situations (homeless/foster care)	<input type="checkbox"/>
	Other indicator information-Please specify:	<input type="checkbox"/>

Category of Data	Elements	Check if used by your system
Student Contact Information	Address	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Phone	<input type="checkbox"/>
Student Identifiers	Local (School district) ID number	<input checked="" type="checkbox"/>
	State ID number	<input type="checkbox"/>
	Vendor/App assigned student ID number	<input type="checkbox"/>
	Student app username	<input type="checkbox"/>
	Student app passwords	<input type="checkbox"/>
Student Name	First and/or Last	<input type="checkbox"/>
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	<input type="checkbox"/>
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	<input type="checkbox"/>
Student Survey Responses	Student responses to surveys or questionnaires	<input type="checkbox"/>
Student work	Student generated content; writing, pictures etc.	<input type="checkbox"/>
	Other student work data -Please specify:	<input type="checkbox"/>
Transcript	Student course grades	<input type="checkbox"/>
	Student course data	<input type="checkbox"/>
	Student course grades/performance scores	<input type="checkbox"/>
	Other transcript data -Please specify:	<input type="checkbox"/>
	Student bus assignment	<input checked="" type="checkbox"/>
	Student pick up and/or drop off location	<input type="checkbox"/>

	Transportation	Student bus card ID number	X
		Other transportation data -Please specify:	<input type="checkbox"/>
	Other	Please list each additional data element used, stored or collected through the services defined in Exhibit A	<input type="checkbox"/>

EXHIBIT "C"

DEFINITIONS

HB 2087: The statutory designation for what is now Texas Education Code Chapter 32 relating to pupil records.

Data: Data shall include, but is not limited to, the following: student data, educational records, employee data, metadata, user content, course content, materials, and any and all data and information that the District (or any authorized end user(s)) uploads or enters through their use of the product. Data also specifically includes all personally identifiable information in education records, directory data, and other non-public information for the purposes of Texas and Federal laws and regulations. Data as specified in Exhibit B is confirmed to be collected or processed by the Operator pursuant to the Services. Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Operator's services.

De-Identified Information (DII): De-Identified Information is Data subjected to a process by which any Personally Identifiable Information ("PII") is removed or obscured in a way that eliminates the risk of disclosure of the identity of the individual or information about them and cannot be reasonably re-identified.

Data Destruction: Provider shall certify to the District in writing that all copies of the Data stored in any manner by Provider have been returned to the District and permanently erased or destroyed using industry best practices to assure complete and permanent erasure or destruction. These industry best practices include, but are not limited to, ensuring that all files are completely overwritten and are unrecoverable. Industry best practices do not include simple file deletions or media high level formatting operations.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, Data, metadata, and user or pupil-generated content obtained by reason of the use of Operator's software, website, service, or app, including mobile apps, whether gathered by Operator or provided by LEA or its users, students, or students' parents/guardians. PII includes Indirect Identifiers, which is any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty. For purposes of this DPA, Personally Identifiable Information shall include the categories of information listed in the definition of Data.

Pupil-Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education 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 pupil content.

Subscribing LEA: A LEA that was not party to the original Services Agreement and who accepts the Operator's General Offer of Privacy Terms.

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

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Operator's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Texas Student Privacy Alliance: The Texas Student Privacy Alliance (TXSPA) is a collaborative group of Texas school districts that share common concerns around student privacy. The goal of the TXSPA is to set standards of both practice and expectations around student privacy such that all parties involved have a common understanding of expectations. The Texas K-12 CTO Council is the organization that sponsors TXSPA and the TXSPA is the Texas affiliate of the National Student Privacy Consortium.

EXHIBIT "D"

SAMPLE REQUEST FOR RETURN OR DELETION OF DATA

Instructions: This Exhibit is optional and provided as a sample ONLY. It is intended to provide a LEA an example of what could be used to request a return or deletion of data.

_____ directs _____ to
LEA OPERATOR

dispose of data obtained by Operator pursuant to the terms of the Service Agreement between
return LEA and Operator. The terms of the Disposition are set forth below:

1. Extent of Return or Disposition

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

Return or Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Return or Disposition

Disposition shall be by destruction or deletion of data.

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

3. Timing of Return or Disposition

Data shall be returned or disposed of by the following date:

As soon as commercially practicable

By the following agreed upon date:

4. Signatures

Authorized Representative of LEA

Date:

5. Verification of Disposition of Data

Authorized Representative of Operator

Date:

EXHIBIT "E"

GENERAL OFFER OF PRIVACY TERMS

Instructions: This is an optional Exhibit in which the Operator may, by signing this Exhibit, be bound by the terms of this DPA to any other Subscribing LEAs who sign the acceptance in said Exhibit. The originating LEA SHOULD NOT sign this Exhibit, but should make Exhibit E, if signed by an Operator, readily available to other Texas K-12 institutions through the TXSPA web portal. Should a Subscribing LEA, after signing a separate Service Agreement with Operator, want to accept the General Offer of Terms, the Subscribing LEA should counter-sign the Exhibit E and notify the Operator that the General Offer of Terms have been accepted by a Subscribing LEA.

1. Offer of Terms

Operator offers the same privacy protections found in this DPA between it and Shutterfly Lifetouch, LLC

and which is dated [11/13/2021] to any other LEA ("Subscribing LEA") who accepts this General Offer through its signature below. This General Offer shall extend only to privacy protections and Operator's signature shall not necessarily bind Operator to other terms, such as price, term, or schedule of services, or to any other provision not addressed in this DPA. The Operator and the other LEA may also agree to change the data provided by LEA to the Operator to suit the unique needs of the LEA. The Operator may withdraw the General Offer in the event of:

- (1) a material change in the applicable privacy statutes;
- (2) a material change in the services and products listed in the Originating Service Agreement;
- (3) the expiration of three years after the date of Operator's signature to this Form.

Operator shall notify the Texas Student Privacy Alliance (TXSPA) in the event of any withdrawal so that this information may be may be transmitted to the Alliance's users.

Operator's Representative:

BY:  _____
E4D02B8212614CC...

Date: 11/13/2021 _____

Printed Name: Andy Panos _____

Title/Position: VP Sales _____

2. Subscribing LEA

A Subscribing LEA, by signing a separate Service Agreement with Operator, and by its signature below, accepts the General Offer of Privacy Terms. The Subscribing LEA and Operator shall therefore be bound by the same terms of this DPA. The Subscribing LEA, also by its signature below, agrees to notify Operator that it has accepted this General Offer, and that such General Offer is not effective until Operator has received said notification.

Subscribing LEA's Representative:

BY: _____

Date: _____

Printed Name: _____

Title/Position: _____

EXHIBIT "F"

DATA SECURITY

1. Operator's Security Contact Information:

Aaron Peck, CISO [Box 26]
Named Security Contact

soc@shutterfly.com (cc: privacy@shutterfly.com) [Box 27]
Email of Security Contact

_____ [Box 28]
Phone Number of Security Contact

2. List of Operator's Subprocessors:

N/A – Lifetouch does not use subprocessors
[Box 29]

3. Additional Data Security Measures:

See Attached Data Security and Privacy Plan [Box 30]



Data Security and Privacy Plan

Shutterfly Lifetouch, LLC ("Lifetouch") is a trusted provider of school services, offering portrait and photography services to schools and families throughout North America since 1936. In preparation for Picture Day, Lifetouch requires certain roster information from your school ("School Data"). This data is used to produce and deliver portrait-based products and services needed for our schools' administrative purposes and/or for use in the school yearbook (the "School Service Items"), to deliver Picture Day notices on behalf of our schools, and to provide parents of students photographed opportunities to purchase portraits. Lifetouch does not use School Data for any unauthorized purposes. As one of the original signatories of the Student Privacy Pledge, Lifetouch is committed to maintaining the security of student data and offering transparency to the schools and families that we serve. This plan outlines how Lifetouch protects School Data in compliance with local, state, and federal privacy law.

Lifetouch complies with federal, state, and local data security and privacy requirements.

As a service provider of staff and student photography for the schools we serve, Lifetouch acknowledges its obligations under the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g, and its implementing regulations, 34 CFR part 99, as well as applicable state student data privacy laws. To perform the services we provide, Lifetouch has a legitimate need for certain School Data to provide photographic services and products for the school's administrative needs. Our schools retain the authority to control Lifetouch's use of School Data, including the right to require the return or destruction of any School Data provided to Lifetouch at any time. Additionally, Lifetouch will strive to meet any additional data handling requirements as prescribed by state or local law, or school district policies, provided we are notified of those requirements before receiving the data. Lifetouch's Privacy Office and Legal Department continually monitor student data privacy laws across the country and work to ensure that Lifetouch remains compliant with these laws.

Lifetouch uses a variety of safeguards to protect School Data.

Lifetouch has implemented a variety of physical, technical, and organizational security measures to help protect School Data from unauthorized access and use.

Facilities. Lifetouch produces portraits and School Service Items within its own U.S.-based photo labs. Lifetouch data, including School Data, is maintained in cloud-based storage or in on-premises data centers that meet or exceed industry standards for cybersecurity. All facilities and systems are protected by strong physical security controls such as restricted role-based access, ID cards, entry logs and video monitoring. We have a secure backup process and utilize high availability systems and equipment to maintain availability.

Lifetouch has robust privacy and security training programs for all employees who handle School Data.

Lifetouch has a robust internal team of dedicated privacy professionals, including the Lifetouch Privacy Office and the Lifetouch Information Security Office, who are responsible for ensuring that Lifetouch employees abide by all relevant laws when handling School Data. Lifetouch also has talented in-house training professionals that routinely hold trainings to educate our employees on privacy laws related to appropriate handling of School Data, as well as our own internal policies and procedures. Our employees complete a variety of in-person and on-demand training programs, including annual data privacy training, and have access to a digital library of reference materials for any questions that may arise. Recordings of live training sessions are also made available for employees to access at any time if they would like additional refreshers.

Lifetouch has a comprehensive response plan for managing data security and privacy incidents and notifying our schools and regulators.

The Lifetouch Privacy Office and Lifetouch Information Security Office work in tandem to maintain a robust incident management program designed to ensure compliance with all statutory and contractual breach notification obligations. Employees are trained to report any actual or suspected incident of unauthorized access to confidential information and the incident management team. When a potential instance of unauthorized access (whether it is a device theft, unauthorized access to a system or database, or some other type of potential compromise), a member of the Lifetouch Information Security Office is responsible for managing the incident. The Information Security Office investigates the incident to confirm if a breach has occurred, manages resolution of the breach, involves the appropriate company staff based on the severity of the incident (including Executive Management, Chief Technology Officer, Legal, HR and Corporate Communications) once a breach has been confirmed, employs all available means to mitigate the breach (for example, remotely disabling a stolen device) and coordinates with Legal to identify reporting responsibilities. Following the incident, the Information Security Office engages the necessary teams to identify any steps to be taken to prevent similar incidents in the future.

Lifetouch securely disposes of school data when it is no longer needed.

School Data is securely destroyed on demand by the school, or in the ordinary course of business when no longer needed to provide school services (typically 18 months following Picture Day), whichever occurs first. School Data storage devices are decommissioned in accordance with the National Institute of Standards and Technology (NIST) SP 800-88 Guidelines for Media Sanitation. Devices and media containing School Data are destroyed or erased using secure deletion methods before being disposed of. Paper copies containing School Data are shredded or otherwise destroyed via a secure disposal vendor.