

**EXHIBIT A - Bill of Rights for Data Security and Privacy**  
**Cheektowaga-Sloan Union Free School District**

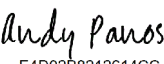
**PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY**

The Cheektowaga-Sloan Union Free School Client is committed to protecting the privacy and security of student data and teacher and principal data. In accordance with New York Education Law Section 2-d and its implementing regulations, the Client informs the school community of the following:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents have the right to inspect and review the complete contents of their child's education records.
3. State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to encryption, firewalls, and password protection, must be in place when data is stored or transferred.
4. A complete list of all student data elements collected by New York State is available for public review at the following website <http://www.nysed.gov/student-data-privacy/student-data-inventory> or by writing to the Office of Information and Reporting Services, New York State Education Department, Room 865 EBA, 89 Washington Avenue, Albany, New York 12234.

**Parents have the right to have complaints about possible breaches of student data addressed.**

**Complaints should be directed in writing to Privacy Complaint, Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website <http://www.nysed.gov/student-data-privacy/form/report-improper-disclosure>.**

CONTRACTOR	
[Signature]	<div style="border: 1px solid black; padding: 2px;"> <small>DocuSigned by:</small>    <small>E4D02B8212614CC...</small> </div>
[Printed Name]	Andy Panos
[Title]	Vice President Sales
Date:	May 3, 2022

## EXHIBIT B

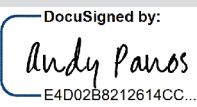
## BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

## SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

<b>Name of Contractor</b>	Shutterfly Lifetouch, LLC
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	School portraits and school service items
<b>Type of PII that Contractor will receive/access</b>	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date 7/01/2022 Contract End Date 7/31/2023
<b>Subcontractor Written Agreement Requirement</b>	Contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) <input checked="" type="checkbox"/> Contractor will not utilize subcontractors. <input type="checkbox"/> Contractor will utilize subcontractors.
<b>Data Transition and Secure Destruction</b>	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> <li>Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.</li> <li>Securely delete and destroy data.</li> </ul>

<b>Challenges to Data Accuracy</b>	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
<b>Secure Storage and Data Security</b>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input checked="" type="checkbox"/> Other:</p> <p>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, IDcards, entry logs and video monitoring. We have a secure backup process and utilize high availability systems and equipment to maintain availability.</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p>
<b>Encryption</b>	Data will be encrypted while in motion and at rest.

CONTRACTOR	
<b>[Signature]</b>	<div>DocuSigned by:</div>  <div>E4D02B8212614CC...</div>
<b>[Printed Name]</b>	Andy Panos
<b>[Title]</b>	Vice President Sales
<b>Date:</b>	May 3, 2022

## EXHIBIT C

**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 New York Education Law § 2-d. 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 (including any Parents Bill of Rights and the school district's Data Security and Privacy Policy implemented pursuant to New York Education Law § 2-d), provided we are notified of such policies 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 will not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose, or otherwise facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

Except for Lifetouch's authorized representatives including its subcontractors or assignees to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the school district, Lifetouch will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student unless required by statute or court order and Lifetouch provides a notice of disclosure to the school district no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

**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.

**Networks.** Devices storing or providing access to School Data are protected with the same multi-layered security strategies that we use to protect Lifetouch's sensitive and confidential business records. Image databases supporting our photo processing labs and websites are separated from associated data files containing identifiable information, and all databases are protected by firewalls, monitoring, vulnerability scanning and authentication procedures. We apply intrusion prevention methods and perform regular network penetration testing and code scanning on a periodic basis using both internal and authorized third party testing services and. Our systems enable secure transmission of School Data from and to the Lifetouch network with encryption technologies. School Data is segregated from other databases in our systems and is securely disposed of when no longer needed. Devices or media containing or accessing School Data are password-protected and encrypted and stored in secure, locked areas when not in use. Laptops and tablets used by our field are also protected by software that, in the event of theft, notifies Lifetouch immediately if the device is connected to any network and allows Lifetouch to remotely erase the device.

**Personnel.** Lifetouch's policy is to collect, use, and disclose personal information only in ways that are consistent with our respect for an individual's privacy. We require Lifetouch employees to sign confidentiality agreements as a condition of employment, and we provide training on the appropriate use and handling of School Data. Access to School Data is limited to those who need it to perform their jobs, and when our employees are instructed to only access School Data secure channels (like the Lifetouch Portal). We also take appropriate measures to enforce these policies.

**Enterprise.** A comprehensive set of IT policies based on ISO 27001/2, PCI-DSS, OWASP and/or NIST frameworks and standards, as applicable, governs information systems practices and procedures throughout the Lifetouch enterprise. Additionally, Lifetouch partners with secure payment processing platforms like PayPal to handle payment card data when the families we serve make their portrait purchases. Additionally, the Lifetouch Portal is designed and maintained to exceed the standards of the Software & Information Industry Association's Best Practices for the Safeguarding of Student Information Privacy and Security for Providers of School Services.

#### **Lifetouch sets strict security requirements for our third-party vendors.**

While Lifetouch does not use third-party contractors to photograph students or manufacture the products we create for our schools and families, Lifetouch does use several vendors to help provide our services (for example, service providers who assist us with data management).

When engaging a new third-party vendor, our information security team completes a brief assessment to determine whether the vendor will have access to any School Data. If so, the team completes an in-depth security questionnaire to evaluate the vendor's information security practices. All Lifetouch vendors who have access to School Data are required to implement the same data privacy commitments that Lifetouch holds our own business to. Each of these vendors then signs an Information Security

Addendum, in addition to their contract with us, that sets out exactly what is required to keep School Data safe, including how the officers and employees of such vendors will be trained on the federal and state laws governing confidentiality of data prior to receiving access to same.

**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 notice 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 release of School Data occurs (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 will promptly notify any school or district whose School Data is subject to unauthorized release without unreasonable delay but no more than seven calendar days after the discovery of such incident.

**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.