Lifetouch

Date:

To: – New York

From: Shutterfly Lifetouch, LLC (**Lifetouch**)

Re: **Photography Agreement Addendum – New York Student Data Privacy and Security**

Lifetouch is aware of the obligations various state and federal laws impose on school service providers who handle school records containing personally identifiable information (PII) of students and teachers. As a trusted provider of school photography for nearly 80 years, Lifetouch has always taken the confidentiality and security of student data very seriously, and we handle such information strictly in accordance with the conditions imposed on "school officials" by the Family Educational Rights in Privacy Act (FERPA).

We want to assure you and confirm that Lifetouch meets and is compliant with all applicable New York State laws, regulations, and NYSED policies. This includes our compliance with the requirements in NY Education Law 2-d and the Parent Bill of Rights.

To that effect, this signed letter, together with the attached signed **Parent Bill of Rights for Data Privacy and Security – New York**, and the attached **Lifetouch Data Security and Privacy Plan**, will serve as an Addendum to the Photography Agreement between your school(s) and Lifetouch.

Please feel free to contact your Lifetouch account representative with any questions or concerns about this important topic. You may also contact the Lifetouch Privacy Office at privacyoffice@lifetouch.com.

SHUTTERFLY LIFETOUCH, LLC

John F. Grant
Vice President - Sales

Lifetouch

Parent Bill of Rights for Data Privacy and Security – New York

Pursuant to Section 2-d of the NY Education Law, parents and students are entitled to certain protections regarding confidential student information.

1. A student's personally identifiable information will not be sold or released for any commercial purposes.

Lifetouch confirms that no PII will be sold or used for marketing or commercial purposes. Under the Photography Agreement between Lifetouch and the District, PII will be limited to that necessary for Lifetouch to perform its duties outlined in the Photography Agreement and the services associated with that function.

2. Parents have the right to inspect and review the complete contents of their child's education record.

See the attached *Lifetouch Data Security and Privacy Plan* for more information about the accuracy of PII collected under the Photography Agreement can be inspected and challenged.

3. Lifetouch is committed to implementing safeguards associated with industry standards and best practice under state and federal laws protecting the confidentiality of personally identifiable information, including but not limited to, encryption, firewalls, and password protection when data is stored or transferred.

See the attached *Lifetouch Data Security and Privacy Plan* for more information about, among other things, (i) how Lifetouch will ensure that any subcontractors or any authorized parties that receive PII will abide by all applicable data protection and security requirements, including but not limited to those outline in applicable state and federal laws and regulations, (ii) what will happen to the PII upon expiration of the Photography Agreement, (iii) where the PII will be stored, how data security will be protected, and the security protections in place to ensure that such data will be protected, including whether such data will be encrypted while in motion and at rest.

4. A complete list of all student data elements collected by New York State is available for public review at http://www.p12.nysed.gov/irs/sirs/ or may be obtained by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

5. Parents have the right to have complaints addressed about possible breaches of student data. Complaints or challenges should be directed to the authorized representative in the District.

SHUTTERFLY LIFETOUCH, LLC

John F. Grant
Vice President Sales

Lifetouch

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 implemented pursuant to New York Education Law § 2-d), 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.

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.

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.