

Central Islip Union Free School District

Program Information and Data Privacy

Third Party Agreement



To be completed **by the vendor** and submitted prior to purchase/implementation. Refusal of the vendor complete this agreement may serve as cause for the district to see similar services through another program and/or vendor. Failure to complete this form in its entirety will significantly delay any/all purchases and payment.

| | |
|---------------------------------------|--|
| VENDOR NAME: | Shutterfly Lifetouch, LLC |
| VENDOR ADDRESS: | 11000 Viking Drive, Eden Prairie, MN 55344 |
| Eastern Suffolk BOCES NYS Contract | <input type="checkbox"/> BOCES Contract <input type="checkbox"/> BOCES CMR <input type="checkbox"/> BOCES Shared-Service <input type="checkbox"/> NYS Contract Pricing. Contract #: <input type="checkbox"/> Federal Contract Pricing. Contract # <input type="checkbox"/> No BOCES/NYS/Federal Contract – Direct Bid/RFP with Vendor |
| PURPOSE | <input checked="" type="checkbox"/> Yearbooks <input checked="" type="checkbox"/> Individual/School/Class Photos <input type="checkbox"/> Fundraiser <input type="checkbox"/> General Sales <input type="checkbox"/> Event/Activity <input type="checkbox"/> OTHER: |
| Personal Information Collected | <input checked="" type="checkbox"/> Names <input checked="" type="checkbox"/> Individual/Group/Class/Club Photos <input checked="" type="checkbox"/> Student ID <input type="checkbox"/> Home Address <input checked="" type="checkbox"/> OTHER: Student school enrollment, Student grade level, Homeroom, Year of Graduation, Parent/Guardian email, Teacher Names, Bus Card ID |

DATA PRIVACY AGREEMENT WITH THE CENTRAL ISLIP UNION FREE SCHOOL DISTRICT

| | |
|---|--|
| Vendor Name: | Shutterfly Lifetouch, LLC |
| Vendor Address: | 11000 Viking Drive, Eden Prairie, MN 55344 |
| Developer/Vendor Privacy Policy Link: | |
| Developer/Vendor Parent Bill of Rights Link | |

This Data Privacy Agreement ("DPA") is by and between the Central Islip Union Free School District (herein known as "EA"), an Educational Agency, and the above listed software, app or extension developer (herein known as "Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

As used in this DPA, the following terms shall have the following meanings:

- Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
- Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
- Disclose:** To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
- Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
- Educational Agency:** As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
- Eligible Student:** A student who is eighteen years of age or older.
- Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.

DS


- 8. NIST Cybersecurity Framework:** The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
- 1. Parent:** A parent, legal guardian or person in parental relation to the Student.
- 2. Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
- 3. Release:** Shall have the same meaning as Disclose.
- 4. School:** Any public elementary or secondary school including a charter school, universal prekindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
- 5. Student:** Any person attending or seeking to enroll in an Educational Agency.
- 6. Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
- 7. Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
- 8. Teacher or Principal APPR Data:** Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

ARTICLE II: PRIVACY AND SECURITY OF PII

9. Compliance with Law.

In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated below ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

10. Authorized Use.

Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.



3. **Data Security and Privacy Plan.**

Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and

Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

1. **EA's Data Security and Privacy Policy**

State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

2. **Right of Review and Audit.**

Upon request by the EA, Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

3. **Contractor's Employees and Subcontractors.**

- (a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. Contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.
- (b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.
- (c) Contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident

^{DS}


in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

- (d) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.
- (a) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. Training.

Contractor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

1. Termination

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

2. Data Return and Destruction of Data.

- (b) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.
- (c) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction.
Redaction is specifically excluded as a means of data destruction.

^{DS}


- (c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.
- (a) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. Commercial or Marketing Use Prohibition.

Contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. Contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. Breach.

- (a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach.

Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

- (b) Notifications required under this paragraph must be provided to the EA at the following address:

Philip K. Voigt
Director of Instructional Technology
50 Wheeler Rd
Central Islip, NY 11722
Pvoigt@centralislip.k12.ny.us

13. Cooperation with Investigations.

Contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. Notification to Individuals.

Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. Termination.

The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. Parent and Eligible Student Access.

Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. Bill of Rights for Data Privacy and Security.

As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. Contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. Priority of Agreements and Precedence.

In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. Execution.

This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.



EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.
2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.
3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 65016502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.
4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.
5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacysecurity/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.
6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA's Director of Technology at pvoigt@centralislip.k12.ny.us (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/reportimproper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to_privacy@nysed.gov; or by telephone at 518-474-0937.
7. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.
8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

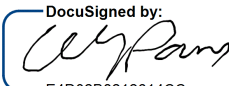


EXHIBIT B - MUST BE COMPLETED IN FULL BY THE VENDOR

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).

| | |
|--|---|
| Description of the purpose(s) for which Contractor will receive/access PII | Description: <i>See attached Photography Agreement Addendum – NY Student Data Privacy and Security</i> <input type="checkbox"/> NO PII OR DATA IS COLLECTED OR VIEWABLE THROUGH THIS PROGRAM/APP |
| Type of PII that Contractor will receive/access | Check all that apply: <i>See attached Photography Agreement Addendum – NY Student Data Privacy and Security</i> |
| Contract Term | Each Contract is valid through the software renewal period or 3 school years in the case of "Free" programs, apps, extensions and pilots. |
| Data Transition and Secure Destruction | Upon expiration or termination of the Contract, Contractor shall: <i>See attached Photography Agreement Addendum – NY Student Data Privacy and Security</i> |
| Challenges to Data Accuracy | 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. |
| Encryption | <i>See attached Photography Agreement Addendum – NY Student Data Privacy and Security</i> |

As the duly authorized officer of the "contractor" as listed above I attest to all of the above submitted information to be true and accept any liability and/or responsibility for any data breaches or intrusions associated with this program, applications, software or browser extension.

DocuSigned by:

F4D02B8212614CC

Signature of Vendor Official Representative

9/25/2021

Date

Signature must be an actual signature and cannot be a script font or text. If the program does not collect or transmit any PII, this document must still be completed, initialed (pages) and signed but you may and the select "NO PII OR DATA IS COLLECTED OR VIEWABLE" option above. No program/app/extension will be considered without a complete agreement.





Date: September 23, 2021

To: Central Islip Union Free School District – 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

A handwritten signature in blue ink, appearing to read "J. Grant", written over a light blue horizontal line.

John F. Grant
Vice President - Sales

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

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.