

**Data Sharing and Confidentiality Agreement (Education Law 2-d Rider)**

**between the**

**ROCKY POINT UNION FREE SCHOOL DISTRICT**

**And**

**IRVIN SIMON PHOTOGRAPHERS**

**146 MEACHAM AVENUE, ELMONT, NEW YORK, 11003 USA**

**IRVIN SIMON PHOTOGRAPHERS provides ID Cards and Individual Student Photos for Rocky Point students and their families.**

Supplemental Agreement dated this 15<sup>th</sup> Day of June 2021 between the ROCKY POINT UNION FREE SCHOOL DISTRICT (the “District”), located at 90 ROCKY POINT-YAPHANK ROAD, ROCKY POINT, NEW YORK, 11778, and IRVIN SIMON PHOTOGRAPHERS (the “Contractor”) are parties to a contract or other written agreement pursuant to which Contractor will receive student data and/or teacher or principal data that is protected under New York Education Law Section 2-d and Part 121 of the Regulations of the Commissioner of Education (collectively referred to as “Section 2-d”) from the District for purposes of providing certain products or services to the District.

WHEREAS, the District and the Vendor have entered into a contract (hereinafter the “Agreement”) whereby the Vendor may receive Student Data or Teacher or Principal Data, as those terms are defined in Education Law §2-d; and

WHEREAS, the Vendor represents that it will only share Protected Information with third party subcontractors if those subcontractors are contractually bound to observe the same obligations to maintain the privacy and security of Protected Information as are required of the Vendor under this Contract and all applicable New York State and Federal laws.

WHEREAS, the District and the Vendor wish to enter into an Agreement in order to comply with Education Law §2-d the Vendor agrees that it will comply with all terms set forth in the Agreement. To the extent that any terms contained in the Agreement, or any terms contained in any other Exhibit(s) attached to and made a part of the Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect. In addition, in the event that the Vendor has online or written Privacy Policies or Terms of Service (collectively, “TOS”) that would otherwise be applicable to its customers or users of the products or services that are the subject of the Agreement between the District and Contractor to the extent that any terms of the TOS, that are or may be in effect at any time during the term of the Master Agreement, conflict with the terms of this Exhibit, the terms of this Exhibit will apply and be given effect.

NOW THEREFORE, in consideration of the mutual promises below, the District and the Vendor agree as follows:

1. **Defined Terms:** Unless otherwise indicated below or elsewhere in this Supplemental Agreement, all capitalized terms shall have the meanings provided in Education Law §2-d.

- a. “Educational Agency” shall generally have the same meaning as the term Educational Agency at Education Law §2-d(1)(c), and in reference to the party to this Agreement shall mean the ROCKY POINT UNION FREE SCHOOL DISTRICT.
  - b. “Third Party Subcontractor” shall mean any person or entity, other than an Educational Agency, that receives Student Data or Teacher or Principal Data from an Educational Agency pursuant to a contract or other written agreement for purposes of providing services to such Educational Agency, including but not limited to data management or storage services, conducting studies for or on behalf of such Educational Agency, or audit or evaluation of publicly funded programs.
  - c. “Protected Data” means Student Data and/or Teacher or Principal Data, to the extent applicable to the product or service actually being provided to the District by Vendor pursuant to the Agreement.
  - d. “Student” means any person attending or seeking to enroll in an Educational Agency.
  - e. “Student Data” means Personally Identifiable Information of a “Student.”
  - f. “Eligible Student” means a Student who is eighteen years or older.
  - g. “Parent” means a parent, legal guardian, or personal in parental relation to a Student.
  - h. “Building Principal” or “Principal” means a building principal subject to annual performance evaluation review under Education Law §3012-c.
  - i. “Classroom Teacher” or “Teacher” means a teacher subject to annual performance evaluation review under Education Law §3012-c.
  - j. “Teacher or Principal Data” means personally identifiable information, as defined in Section 2-d, relating to the annual professional performance reviews of classroom teachers or principals that Vendor may receive from the District pursuant to the Agreement..
  - k. “Personally Identifiable Information” shall have the following meanings:
    - i. As applied to Student Data, shall mean Personally Identifiable Information as defined in 34 CFR 99.3 implementing the Family Educational Rights and Privacy Act (FERPA)
    - ii. As applied to Teacher or Principal Data, shall mean Personally Identifiable Information as that term is defined in Education Law §3012c.
  - l. “NIST Cybersecurity Framework” means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).
2. The District has developed the **Parents’ Bill of Rights for Data Privacy and Security**, the terms of which are applicable to the Agreement between the District and the Vendor and are incorporated into this Supplemental Agreement. The Parents Bill of Rights for Data Privacy and Security states:
    - a. A student's personally identifiable information cannot be sold or released for any commercial purposes.
    - b. Parents have the right to inspect and review the complete contents of their child's

education record maintained by the Rocky Point Union Free School District.

- c. State and federal laws protect the confidentiality of personally identifiable information. 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.
- d. A complete list of all student data elements collected by the State is available for public review at  
<http://www.p12.nysed.gov/irs/sirs/documentation/NYSEDstudentData.xlsx>  
or a copy may be obtained by writing to:  
Office of Information & Reporting Services  
New York State Education Department, Room 863 EBA 89  
Washington Avenue  
Albany, NY 12234
- e. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to:  
Aaron Factor, Executive Director of Curriculum, Technology, & Innovation  
Rocky Point UFSD  
90 Rocky Point-Yaphank Road  
Rocky Point, NY, 11778  
631-849-7080 [afactor@rockypoint.k12.ny.us](mailto:afactor@rockypoint.k12.ny.us)
- f. “Supplemental information” for each contract into which the District enters with a third party who receives student data or teacher or principal data shall:
  - i. The exclusive purposes for which the student data or teacher or principal data will be used;
  - ii. How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
  - iii. When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
  - iv. If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
  - v. Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
- g. This Bill of Rights is subject to change based on regulations of the Commissioner of Education and the New York State Education Department’s Chief Privacy Officer, as well as emerging guidance documents.

3. As required by Education Law §2-d(3)(c), the District has developed the following

“supplemental information” for the Agreement with the Vendor:

- a. Student Data and/or Teacher or Principal Data which the Vendor comes into possession as part of its Agreement with the District shall be used for the exclusive purpose(s) of performing Contractor’s obligations under this Agreement.
- b. The Vendor will ensure that any and all subcontractors, persons or entities that the Vendor may share the Student Data and/or Principal or Teacher Data with will abide by the terms of the Agreement, this Supplemental Agreement, and/or the data protection and security requirements set forth in Education Law §2-d.
- c. When the Agreement terminates between the District and the Vendor, the Vendor shall return such data to the District or if agreed to by the District, destroy the remaining Student Data and/or Principal or Teacher Data that the Vendor still maintains in any form in a manner agreeable to the district.
- d. Any challenges concerning the accuracy of Student Data and/or Principal Data shall be handled directly between the District and the Parent, Student, Eligible Student, Teacher or Principal. The Vendor agrees to abide by the outcome of such challenges and make any corrections and/or changes to the applicable Student Data and/or Principal or Teacher Data as determined by the District.”
- e. The District and the Vendor hereby agree that the Student Data and/or Principal or Teacher Data shall be stored in the following manner:

*[The Vendor to attach a detailed procedure in which Student Data and/or Principal or Teacher Data will be stored, and the security procedures that will be taken to ensure that the Data will be protected, and provide information on how the data will be encrypted.]*

4. As required by Education Law §2-d(5)(e), the Vendor hereby agrees that any officers or employees of the Vendor, including any third-party subcontractors or assignees, who have access to Student Data or Teacher or Principal Data will have or will receive training on the Federal and New York State laws governing confidentiality of Student Data and/or Principal or Teacher Data prior to receiving access.

*[The Vendor to attach a detailed document specifying how employees and its assignees receive or will receive training on the laws governing data prior to receiving access to the data. The Vendor should indicate in this document if they will use sub-contractors and how it will manage the subcontractor relationships and contracts.]*

5. As required by Education Law §2-d(5)(f), the Vendor hereby agrees that it shall:
  - a. Limit internal access to education records to those individuals that are determined to have legitimate educational interests;
  - b. Not use the educational records for any other purposes than those explicitly authorized in the Agreement or this Supplemental Agreement;
  - c. Except for authorized representatives of the Vendor to the extent they are carrying out the Agreement or this Supplemental Agreement, not disclose any Personally Identifiable Information to any other party:

- i. Without the prior written consent of the Parent or Eligible Student; or
    - ii. Unless required by statute or court order and the party provides a notice of the disclosure to the State Education Department, District Board of Education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order.
  - d. Maintain administrative, technical, and physical safeguards that equal industry best practices including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection, and that align with the NIST Cybersecurity Framework 1.0;
  - e. Store all data in the continental United States (CONUS) or Canada.
  - f. Vendor will use encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the secretary of the U.S. Department of HHS in guidance issued under P.L. 111-5, Section 13402(H)(2).
6. Breach and unauthorized release of Personally Identifiable Information:
- a. In accordance with Education Law §2-d(6), the Vendor shall be required to notify the District of any breach of security resulting in an unauthorized release of Student Data and/or Principal or Teacher Data by the Vendor or its subcontractors or assignees in violation of applicable state or federal law, the Parents Bill of Rights for Student Data Privacy and Security, the data privacy and security policies of the District and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay. The District shall, upon notification by the Vendor, be required to report to the Chief Privacy Officer, who is appointed by the State Education Department, any such breach of security and unauthorized release of such data.
  - b. In the case of an unauthorized release of Student Data, the District shall notify the Parent or Eligible Student of the unauthorized release of Student Data that includes Personally Identifiable Information from the student records of such Student in the most expedient way possible and without unreasonable delay. In the case of an unauthorized release of Teacher or Principal Data, the District shall notify each affected Teacher or Principal of the unauthorized release of data that includes Personally Identifiable Information from the Teacher or Principal's annual professional performance review in the most expedient way possible and without unreasonable delay.
  - c. To cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Protected Data.
  - d. In the case of notification to a Parent, Eligible Student, Teacher or Principal due to the unauthorized release of student data by the Vendor, or its subcontractors or assignees, the Vendor shall promptly reimburse the educational agency for the full cost of such notification, as required by Education Law §2-d(6)(c).

*[Attach a document specifying how the Vendor will manage incidents including specifying any plans to identify incidents, and to notify the District.]*

7. Miscellaneous:

- a. The District and Contractor agree that if applicable laws change and/or if the Commissioner of Education implements Regulations which affects the obligations of the parties herein, this Agreement shall be deemed to incorporate such changes as necessary in order for the District and the Vendor to operate in compliance with the amendment or modified requirements under the applicable laws or regulations.
- b. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the District to comply with the applicable laws or regulations.
- c. Nothing express or implied in this Agreement is intended to confer upon any person other than the District, Contractor and their respective successors and assigns any rights, remedies, obligations or liabilities.
- d. **This agreement expires June 30, 2022.** Upon expiration of this Contract without a successor agreement in place, the Vendor shall assist the Rocky Point Union Free School District in exporting all Protected Information previously received from, or then owned by the Rocky Point Union Free School District.
- e. Upon expiration of this Contract with a successor agreement in place, the Vendor will cooperate with the Rocky Point Union Free School District as necessary to transition protected data to the successor vendor prior to deletion. The Vendor shall thereafter securely delete and overwrite any and all Protected Information remaining in the possession of the Vendor or its assignees or subcontractors (including all hard copies, archived copies, electronic versions or electronic imaging of hard copies of shared data) as well as any and all Protected Information maintained on behalf of the Vendor in secure data center facilities.
- f. The Vendor shall ensure that no copy, summary or extract of the Protected Information or any related work papers are retained on any storage medium whatsoever by the Vendor, its subcontractors or assignees, or the aforementioned secure data center facilities.

**IN WITNESS WHEREOF**, the Parties hereto have duly executed this Agreement.

BY THE VENDOR: **IRVIN SIMON PHOTOGRAPHERS**

Stephen Miller  
Name (Print)

Stephen Miller  
Signature

President  
Title

6.8.21  
Date



**irvin simon**

PHOTOGRAPHERS

## **New York State Student Data Privacy and Security**

Irvin Simon Photographers 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 over 75 years, Irvin Simon 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 Irvin Simon Photographers 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 **Irvin Simon Data Security and Privacy Plan**, will serve as an Addendum to the Photography Agreement between your school(s) and Irvin Simon Photographers.

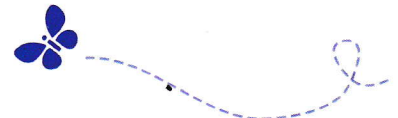
Please feel free to contact your Irvin Simon Account Manager with any questions or concerns about this important topic.

Sincerely,

*Eric M. Miller, CTO*

Irvin Simon Photographers

146 Meacham Avenue  
Elmont, New York 11003  
Office 800.540.4701  
Fax 516.437.0158



smiles you can count on  
irvinsimon.com

**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. Irvin Simon Photographers confirms that no PII will be sold or used for marketing or commercial purposes other than what is necessary for Irvin Simon 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 *Irvin Simon Photographers Data Security and Privacy Plan* for more information about the accuracy of PII collected under the Photography Agreement can be inspected and challenged.
3. Irvin Simon Photographers 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 *Irvin Simon Data Security and Privacy Plan* for more information about, among other things, (i) how we 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 outlined in applicable state and federal law 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.





## **Data Security and Privacy Plan**

Irvin Simon Photographers ("Irvin Simon") is a trusted provider of school services, offering portrait and photography services to schools and families since 1946. In preparation for Picture Day, Irvin Simon 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. Irvin Simon does not use School Data for any unauthorized purposes. Irvin Simon is committed to maintaining the security of student data and offering transparency to the schools and families that we serve. This plan outlines how Irvin Simon protects School Data in compliance with local, state, and federal privacy law.

### **Irvin Simon 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, Irvin Simon 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, Irvin Simon 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 Irvin Simon's use of School Data, including the right to require the return or destruction of any School Data provided to Irvin Simon at any time. Additionally, Irvin Simon 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.

### **Irvin Simon uses a variety of safeguards to protect School Data.**

Irvin Simon has implemented a variety of physical, technical, and organizational



# irvin simon

## PHOTOGRAPHERS

security measures to help protect School Data from unauthorized access and use.

Facilities. Irvin Simon data, including School Data, is maintained in cloud-based storage or in our on-premises data center 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, 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 Irvin Simon'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 Irvin Simon 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 Irvin Simon immediately if the device is connected to any network and allows Irvin Simon to remotely erase the device.

Personnel. Irvin Simon'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 Irvin Simon 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. We also take appropriate measures to enforce these policies.



**irvin simon**

PHOTOGRAPHERS

Enterprise. Irvin Simon partners with secure payment processing platforms like Shopify to handle payment card data when the families we serve make their portrait purchases. Additionally, all customer interface 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.

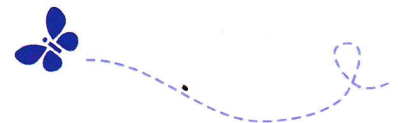
**Irvin Simon has a comprehensive response plan for managing data security and privacy incidents and notifying our schools and regulators.**

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), our Chief Technology Office (CTO) is responsible for managing the incident. The CTO 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, once a breach has been confirmed, employs all available means to mitigate the breach and coordinates to identify reporting responsibilities. Following the incident, the CTO engages the necessary teams to identify any steps to be taken to prevent similar incidents in the future. Irvin Simon 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.

**Irvin Simon 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, 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.

146 Meacham Avenue  
Elmont, New York 11003  
Office 800.540.4701  
Fax 516.437.0158



smiles you can count on  
irvinsimon.com