

CAZENOVIA
CENTRAL SCHOOL DISTRICT



**A TRADITION OF
EXCELLENCE & EQUITY**

31 Emory Ave
Cazenovia, NY 13421

JENNIFER RAUX
Director of Instructional Technology

Phone: 315.655.1314, X.5380

DATE: 9-14-23

To Whom it May Concern:

RE: <BJK Photos> Agreement with Cazenovia Central School District

The Cazenovia Central School District would like to contract with your company for the above referenced program/service. Attached you will find the agreement between your company and the Cazenovia Central School District concerning the NYS Ed Law and Regulations 121, Data Security and Privacy. Please review the agreement and return signed to Jennifer Raux, Director of Instructional Technology via email.

Sincerely,

Jennifer Raux
Director of Instructional Technology, Data Protection Officer
Cazenovia Central School District
31 Emory Ave
Cazenovia, NY 13035
jraux@caz.cnyric.org
315-655-1314 ext. 5380

Cazenovia Central School District

Data Security and Privacy Contract & Parents' Bill of Rights

Pursuant to Section 2-d of the Education Law, agreements entered into between the District and a third-party contractor which require the disclosure of student data and/or teacher or principal data that contains personally identifiable information ("PII") to the contractor, must include a data security and privacy plan and must ensure that all contracts with third-party contractors incorporate the District's Parents' Bill of Rights for Data Security and Privacy.

As such, BJK Photos _____ ("the Contractor") agrees that the following terms shall be incorporated into the contract for services ("the Contract") and it shall adhere to the following:

1. The Contractor's storage, use and transmission of student and teacher/principal PII shall be consistent with the District's Data Security and Privacy Policy available here:
 - a. <http://go.boarddocs.com/ny/cazenovia/Board.nsf/goto?open&id=CBQJDW4CBE06>
2. Contractor shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.
3. The exclusive purposes for which the student data or teacher or principal data will be used under the contract are set forth in Paragraph __ of the Vendor Privacy Policy/Contract only for the term of the Contract as set forth in Paragraph ____ or as summarized below.
4. The Contract shall maintain the following administrative, operational and technical safeguards and practices in place to protect PII, which shall align with the NIST Cybersecurity Framework, including:
 - a. PII data will be protected using encryption while in motion and at rest. Please describe:

See Attached

- b. PII will be stored in a manner as to protect its security and to mitigate any potential security risks. Specifically, all student data and/or teacher or principal data will be stored as follows:

See Attached

The security of this data will be ensured by:

See Attached

Cazenovia Central School District

- c. Physical access to PII by individuals or entities described in paragraph 3 above shall be controlled as follows:

See Attached

- 5. The Contractor shall ensure that no PII is disclosed to employees, subcontractors, or other persons or entities unless they have a legitimate educational interest and only for purposes necessary to provide services under the Contract.

- a. By initialing here JK_____, the Contractor represents that it will not utilize any subcontractors or outside entities to provide services under the Contract and shall not disclose any PII other than as required pursuant to paragraph 6 below.

- b. If subcontractors are used, describe how the Contractor will manage data privacy and security:

See Attached

- 6. Contractor shall ensure that all employees, subcontractors, or other persons or entities who have access to PII will abide by all applicable data protection and security requirements, including, but not limited to those outlined in applicable laws and regulations (e.g., FERPA, Education Law Section 2-d). Contractor shall provide training to any employees, subcontractors, or other persons or entities to whom it discloses PII as follows:

See Attached

- 7. Contractor shall not disclose PII to any other party other than those set forth in paragraph 4 above without prior written parental consent or unless required by law or court order. If disclosure of PII is required by law or court order, the Contractor shall notify the New York State Education Department and the District no later than the time the PII is disclosed unless such notice is expressly prohibited by law or the court order.

Cazenovia Central School District

8. Upon expiration of the contract, the PII will be returned to the District and/or destroyed. Describe below the transfer and/or destruction information (i.e., whether, when and in what format the data will be returned to the District, and/or whether, when and how the data will be destroyed.

See attached

9. The parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data collected in accordance with the procedures set forth in the FERPA regulations at 99 C.F.R. Part 34, Subpart C, §§99.20-99.22.
10. The Contractor shall take the following steps to identify breaches or unauthorized releases of PII and to notify the District upon learning of an unauthorized release of PII. Minimum requirements are noted below in 10a, 10b and 10c.
 - a. Provide prompt notification to the District no later than seven (7) calendar days from date of discovery of a breach or unauthorized release of PII. Contractor shall provide notification to the District's data privacy officer by phone and by email.
 - b. Contractor shall cooperate with the District and law enforcement to protect the integrity of the investigation of any breach or unauthorized release of PII.
 - c. Where a breach or unauthorized release is attributed to the Contractor, the Contractor shall pay for or promptly reimburse the District for the full cost of such notification.
11. 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 parents may obtain a copy of this list by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.
12. Parents have the right to file complaints with the District about possible privacy breaches of student data by the District's third-party contractors or their employees, officers, or assignees, or with NYSED. Complaints to NYSED should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to CPO@mail.nysed.gov.

Cazenovia Central School District

AGREED TO BY:

Organization: BJK Photos


Contractor's Signature: Janet King

Name: Janet King

Title: VP Operations/Co-Owner

Date: 9/14/23

District: Cazenovia Central School District

Administrator's Signature: 

Name: Jennifer Raux

Title: Director of Instructional Technology

Date: 9-15-23

Cazenovia Central School District

PARENTS' BILL OF RIGHTS – SUPPLEMENTAL INFORMATION ADDENDUM E

1. **EXCLUSIVE PURPOSES FOR DATA USE:** The exclusive purposes for which “student data” or “teacher or principal data” (as those terms are defined in Education Law Section 2-d and collectively referred to as the “Confidential Data”) will be used by [insert name of third-party contractor] (the “”) are limited to the purposes authorized in the contract between the Vendor and Cazenovia Central School District (the “School District”) dated [insert contract date] (the “Contract”).
2. **SUBCONTRACTOR OVERSIGHT DETAILS:** The Vendor will ensure that any subcontractors, or other authorized persons or entities to whom the Vendor will disclose the Confidential Data, if any, are contractually required to abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable state and federal laws and regulations (e.g., Family Educational Rights and Privacy Act (“FERPA”); Education Law §2-d; 8 NYCRR Part 121).
3. **CONTRACT PRACTICES:** The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to the School District in [insert data format] format and/or destroyed by the Vendor as directed by the School District.
4. **DATA ACCURACY/CORRECTION PRACTICES:** A parent or eligible student can challenge the accuracy of any “education record”, as that term is defined in the FERPA, stored by the School District in a Vendor’s product and/or service by following the School District’s procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by School District in Vendor’s product and/or service by following the appeal procedure in the School District’s APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.
5. **SECURITY PRACTICES:** Confidential Data provided to Vendor by the School District will be stored [insert location]. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework including, but not necessarily limited to, disk encryption, file encryption, firewalls, and password protection.
6. **ENCRYPTION PRACTICES:** The Vendor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

This Agreement, made this September 14, 2023 ("Effective Date"), by and between the Cazenovia Central School District ("School District"), having an office at and BJK Photos, LLC. having an address at 181 Kenwood Ave. Oneida, NY 13421 (collectively the "Parties").

In consideration of the mutual promises and covenants contained herein, the Parties agree as follows:

1. Services. Vendor hereby grants to School District, including to all School District's authorized users, a non-exclusive, non-sublicensable, non-assignable and royalty-free license to access and use the service(s) and/or program(s). The Vendor shall further perform related services and any additional services as set forth in Addendum C (collectively, "Services"). Vendor shall provide the Services at the School District location or on a remote basis, as agreed to by the Parties. Vendor warrants that the Services provided hereunder will be performed in a good and workmanlike manner.

2. Term of Services. This Agreement begins on the Effective Date and will continue for one year unless terminated earlier as set forth herein (the "Term").

3. Termination. This Agreement may be terminated as follows:

- (a) By the School District upon thirty (30) days' prior written notice to Vendor.
- (b) By the School District immediately in the event of breach by the Vendor.
- (c) By either Party in the event of a Default not cured within the time period set forth in Section 7 herein; and
- (d) By either Party upon written mutual agreement.

4. Payment. Payment shall be made in accordance with Addendum D attached hereto.

5. Protection of Confidential Data. Vendor shall provide its Services in a manner which protects Student Data (as defined by 8 NYCRR 121.1 (q)) and Teacher or Principal Data (as defined by 8 NYCRR 121.1 (r)) (hereinafter "Confidential Data") in accordance with the requirements articulated under Federal, State, and local laws and regulations, including but not limited to the foregoing:

- (a) Vendor will adopt technologies, safeguards and practices that align with the NIST Cybersecurity Framework.
- (b) Vendor will comply with the School District Data Security and Privacy Policy, Education Law 2-d, and 8 NYCRR 5121.
- (c) Vendor will limit internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services.
- (d) Vendor will not use the personally identifiable information for any purpose not explicitly authorized in this Agreement.
- (e) Vendor will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student, unless otherwise authorized pursuant to applicable law.

- (f) Vendor will maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of personally identifiable information in its custody.
- (g) Vendor will use encryption to protect personally identifiable information in its custody while in motion or at rest.
- (h) Vendor will not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

In the event Vendor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the Vendor shall apply to the subcontractor.

6. Data Breach. In the event that Confidential Data is accessed or obtained by an unauthorized individual, Vendor shall provide notification to the School District without unreasonable delay and not more than seven calendar days after the discovery of such breach. Vendor shall follow the following process:

- (a) The security breach notification shall be titled "Notice of Data Breach," shall be clear, concise, use language that is plain and easy to understand, and to the extent available, shall include: a brief description of the breach or unauthorized release; the dates of the incident and the date of discovery; a description of the types of Confidential affected; an estimate of the number of records affected; a brief description of the vendors investigation or plan to investigate; and contact information for representatives who can assist the School District with additional questions.
- (b) The Vendor shall also prepare a statement for parents and eligible students which provides information under the following categories: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information."
- (c) Where a breach or unauthorized release of Confidential Data is attributed to Vendor, and/or a subcontractor or affiliate of Vendor, Vendor shall pay for or promptly reimburse the School District for the cost of notification to parents and eligible students of the breach.
- (d) Vendor shall cooperate with the School District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of Confidential Data.
- (e) Vendor further acknowledges and agrees to have a written incident response plan that is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Protected Data or any portion thereof. Upon request, Vendor shall provide a copy of said written incident response plan to the School District.

7. Indemnification. Vendor shall at all times (both during and after the Term of this Agreement), indemnify, defend and hold harmless the School District, its agents, employees and students (collectively for purposes of this Section "the School District"), from and against any and

all settlements, losses, damages, costs, counsel fees and all other expenses relating to or arising from (a) Vendor's failure to comply with the terms of this Agreement; and/or (b) the negligent operations, acts or omissions of the Vendor.

Without intending to create any limitation relating to the survival of any other provisions of this Agreement, Vendor and Client agree that the terms of this paragraph shall survive the expiration or earlier termination of this Agreement. Each party shall promptly notify the other in the event of the threat or initiation of any claim, demand, action or proceeding to which the indemnification obligations set forth in this Section may apply.

8. Assignment. This Agreement is binding upon the Parties and their respective successors and assigns, but Vendor's obligations under this Agreement are not assignable without the prior written consent of the School District. Any assignment without the School District's consent shall be null and void.

9. Default. The School District shall be in Default under this Agreement if the School District fails to pay any fees or charges, or any other payments required under this Agreement when due and payable, and such failure continues for a period of fifteen (15) days after receipt of written notification of such failure. The Vendor shall be in default of this

Agreement if it becomes insolvent, dissolves, or assigns its assets for the benefit of its creditors, or files or has filed against it any bankruptcy or reorganization proceeding.

10. Intellectual Property. Intellectual property rights arising from the Services (but not the data, materials or content provided by Client) shall remain the property of Vendor, and nothing contained in any work product shall be construed to transfer, convey, restrict, impair or deprive Vendor of any of its ownership or proprietary interest or rights in technology, information or products that existed prior to the provision of deliverables under this Agreement or that may be independently developed by Vendor outside the scope of the services provided under this Agreement and without use of any confidential or otherwise restricted material or information thereunder.

11. Governing Law. This Agreement and any Services procured hereunder shall be governed by the laws of the State of New York both as to interpretation and performance, without regard to its choice of law requirements. Each party consents and submits, for any dispute arising out of or relating to this Agreement or the transactions contemplated hereby, to the sole and exclusive jurisdiction of the state and federal courts located in the county in which the School District is located.

12. Compliance with Laws. Vendor, its employees, and representatives shall at all times comply with all applicable Federal, State and local laws, rules and regulations.

13. Independent Relationship. It is expressly intended by the Parties hereto, and Vendor hereby specifically warrants, represents, and agrees, that Vendor and the School District are independent entities. The Parties intend that this Agreement is strictly between two independent entities and does not create an employer/employee relationship for any purpose. Vendor shall perform the duties contemplated by this Agreement as an independent entity, to whom no benefits shall accrue except for those benefits expressly set forth in this Agreement.

14. Public Inspection of Agreement. Vendor acknowledges and agrees that this Agreement and all documents Vendor provides to School District as required herein, are public records and may at all times be subject to public inspection.

15. Waiver. No delay or omission of the School District to exercise any right hereunder shall be construed as a waiver of any such right and the School District reserves the right to exercise any such right from time to time, as often as may be deemed expedient.

16. Addendums. The following Addendums are attached hereto and incorporated herein:

- Addendum A: Parents' Bill of Rights for Data Privacy and Security
- Addendum B: Parents' Bill of Rights — Supplemental Information Addendum
- Addendum C: Product Specifications and Pricing Table
- Addendum D: Vendor's Data Security and Privacy Plan
- Addendum E: Schedule of Data

17. Severability. Should any part of this Agreement for any reason be declared by any court of competent jurisdiction to be invalid, such decision shall not affect the validity of any remaining portion, which remaining portion shall continue in full force and effect as if this Agreement had been executed with the invalid portion thereof eliminated, it being the intention of the Parties that they would have executed the remaining portion of this Agreement without including any such part, parts or portions which may for any reason be hereafter declared invalid.

18. Entire Agreement. This Agreement and its attachment constitute the entire Agreement between the Parties with respect to the subject matter hereof and shall supersede all previous negotiations, commitments, and writings. It shall not be released, discharged, changed, or modified except by an instrument in writing signed by a duly authorized representative of each of the Parties.

19. Renewal of Agreement. Upon the expiration of the original term or any renewal term, this Services Agreement shall be automatically renewed for another one (1) year period unless, at least thirty (30) day prior to the renewal date, the District gives the other party written notice of its intent not to renew. During any renewal term of employment, the terms, conditions, and provisions set forth in this Services Agreement shall remain in effect unless modified in accordance with the Services Agreement.

IN WITNESS WHEREOF, the parties have executed this Agreement intending to be
legally bound.

School District

BJK Photos,
LLC

Signature

Elizabeth Jones

President

Title

Addendum A

PARENTS' BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

The Common Core Implementation Reform Act enacted in 2014 requires school districts and BOCES to publish a Parents Bill of Rights for Data Privacy and Security. The following constitutes the School District's Bill of Rights for privacy of student data. 1 . A

student's personally identifiable information (PII) cannot be sold or released for any commercial purpose. PII, as defined by Education Law 2-d and 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, 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); 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-privacy-security, 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. Complaints may be submitted to NYSED at www.nysed.gov/data-privacy-security; by mail to: Jennifer Raux Cazenovia Central School District 31 Emory Street Cazenovia, NY 13035
7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
8. 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.
9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

Addendum B

PARENTS' BILL OF RIGHTS - SUPPLEMENTAL INFORMATION ADDENDUM

1. As used in this Addendum B, the following terms will have the following meanings:
 - a. "Student" shall have the meaning defined in Subsection I(f) of Section 2-d.
 - b. "Eligible Student" shall have the meaning defined in Subsection 1 (g) of Section 2-d.
 - c. "Personally Identifiable Information" as applied to Student Data shall have the meaning defined in Subsection 1 (d) of Section 2-d.
 - d. "Student Data" means Personally Identifiable Information from student records that Vendor receives from School District.

Other capitalized terms used in this Addendum B will have the applicable meaning set forth elsewhere in this Agreement or in Section 2-d.

2. Vendor agrees that the confidentiality of Student Data shall be maintained in accordance with state and federal laws that protect the confidentiality of Student Data.
3. Vendor agrees that any of its officers or employees, and any officers or employees of any assignee of Vendor, who have access to Student Data will be provided training on the federal and state law governing confidentiality of such Student Data prior to receiving access to that data.
4. The exclusive purpose for which Vendor is being provided access to Student Data is to permit Vendor to provide Services as set forth in the Agreement. Student Data received by Vendor, or by any assignee of Vendor or third party contracting with Vendor, shall not be sold or used for marketing purposes.
5. If Vendor comes into possession of Student Data, Vendor will only share such Student Data with additional third parties if those third parties are contractually bound to adhere to data protection and security requirements, including but not limited to those outlined in applicable state

and federal laws and regulations (e.g., Family Educational Rights and Privacy Act ("FERPA"), Education Law § 8 NYCRR Part 121).

6. The Contract commences and expires on the dates set forth in the Contract, unless earlier terminated or renewed pursuant to the terms of the Contract. On or before the date the Contract expires, protected data will be exported to School District and/or destroyed by the Contractor as directed by School District

7. If a parent, Student, or Eligible Student wishes to challenge the accuracy of any "education record", as that term is defined in the FERPA, by following the School District's procedure for requesting the amendment of education records under the FERPA. Teachers and principals may be able to challenge the accuracy of APPR data stored by School District in Contractor's product and/or service by following the appeal procedure in the School District's APPR Plan. Unless otherwise required above or by other applicable law, challenges to the accuracy of the Confidential Data shall not be permitted.

8. Student Data transferred to Vendor by School District will be stored in electronic memory (on servers or other computers) operated and maintained by or on behalf of Vendor in the United States. The measures that Vendor will take to protect the privacy and security of Student Data while it is stored in that manner include, but are not necessarily limited to: encryption to the extent required by Section 2-d; restricted physical access to the servers/computers; software-based solutions intended to prohibit unauthorized entry such as regularly updated virus scans, firewalls, and use of passwords; and administrative controls such as selective user access rights. The measures that Vendor takes to protect Confidential Data will align with the NIST Cybersecurity Framework.

9. The Contractor will apply encryption to the Confidential Data while in motion and at rest at least to the extent required by Education Law Section 2-d and other applicable law.

Addendum C

PRIVACY POLICY & Data Security Policy

WEBSITE AND EMAIL PRIVACY POLICY TEMPLATE

Last updated March 2020

INTRODUCTION

BJK Photos, LLC ("we" or "us" or "our") respects the privacy of our users ("user" or "you"). This Privacy Policy explains how we collect, use, disclose, and safeguard your information when you visit our BJK Photos.com including any other media form, media channel, mobile website, or mobile application related or connected thereto (collectively, the "Site"). Please read this privacy policy carefully. If you do not agree with the terms of this privacy policy, please do not access the site.

We reserve the right to make changes to this Privacy Policy at any time and for any reason. We will alert you about any changes by updating the "Last Updated" date of this Privacy Policy. Any changes or modifications will be effective immediately upon posting the updated Privacy Policy on the Site, and you waive the right to receive specific notice of each such change or modification.

You are encouraged to periodically review this Privacy Policy to stay informed of updates. You will be deemed to have been made aware of, will be subject to, and will be deemed to have accepted the changes in any revised Privacy Policy by your continued use of the Site after the date such revised Privacy Policy is posted. This template was created using Termly' Privacy Policy Generator.

COLLECTION OF YOUR INFORMATION

We may collect information about you in a variety of ways. The information we may collect on the Site includes:

Personal Data

Personally identifiable information, such as your name, shipping address, email address, and telephone number, and demographic information, such as your age, gender, hometown, and interests, that you voluntarily give to us on bjkphotos.com or when you choose to participate in various activities related to bjkphotos.com, such as online chat and message boards and subscription to newsletters and promotional emails. You are under no obligation to provide us with personal information of any kind, however your refusal to do so may prevent you from using certain features of the bjkphotos.com

Derivative Data

Information our servers automatically collect when you access the Site, such as your IP address, your browser type, your operating system, your access times, and the pages you have viewed directly before and after accessing the Site.

Financial Data

Financial information, such as data related to your payment method (e.g. valid credit card number, card brand, expiration date) that we may collect when you purchase, order, return, exchange, or request information about our services is not stored or accessible after the transaction is processed.

Facebook Permissions

The Site may by default access your Facebook basic account information, including your name, email, gender, birthday, current city, and profile picture URL, as well as other information that you choose to make public. We may also request access to other permissions related to your account, such as friends, check-ins, and likes, and you may choose to grant or deny us access to each individual permission. For more information regarding Facebook permissions, refer to the Facebook Permissions Reference page.

Mobile Device Data

Device information, such as your mobile device ID, model, and manufacturer, and information about the location of your device, if you access the Site from a mobile device.

Data from Contests, Giveaways, and Surveys

Personal and other information you may provide when entering contests or giveaways and/or responding to surveys.

USE OF YOUR INFORMATION

Having accurate information about you permits us to provide you with a smooth, efficient, and customized experience. Specifically, we may use information collected about you via the bjkphotos.com to:

- Administer sweepstakes, promotions, and contests.
- Compile anonymous statistical data and analysis for use internally or with third parties.
 - Create and manage your account.
- Deliver targeted advertising, coupons, newsletters, and other information regarding promotions and the Site [and our mobile application] to you.
 - Email you regarding your account or order.
 - Enable user-to-user communications.
- Fulfill and manage purchases, orders, payments, and other transactions related to bjkphotos.com
- Generate a personal profile about you to make future visits to the Site more personalized.
 - Increase the efficiency and operation of the Site
 - Monitor and analyze usage and trends to improve your experience with the Site.
 - Notify you of updates to the Site.
- Offer new products, services, [mobile applications,] and/or recommendations to you.
 - Perform other business activities as needed.
- Prevent fraudulent transactions, monitor against theft, and protect against criminal activity.
 - Process payments and refunds.
 - Request feedback and contact you about your use of the Site.
 - Resolve disputes and troubleshoot problems.
 - Respond to product and customer service requests.
 - Send you a newsletter
 - Solicit support for the Site.

DISCLOSURE OF YOUR INFORMATION

We may share information we have collected about you in certain situations. Your information may be disclosed as follows:

By Law or to Protect Rights

If we believe the release of information about you is necessary to respond to legal process, to investigate or remedy potential violations of our policies, or to protect the rights, property, and safety of others, we may share your information as permitted or required by any applicable law, rule, or regulation. This includes exchanging information with other entities for fraud protection and credit risk reduction.

Third-Party Service Providers

We may share your information with third parties that perform services for us or on our behalf, including payment processing, data analysis, email delivery, hosting services, customer service, and marketing assistance.

Online Postings

When you post comments, contributions or other content to the Site your posts may be viewed by all users and may be publicly distributed outside the Site in perpetuity.

Affiliates

We may share your information with our affiliates, in which case we will require those affiliates to honor this Privacy Policy. Affiliates include our parent company and any subsidiaries, joint venture partners or other companies that we control or that are under common control with us.

Business Partners

We may share your information with our business partners to offer you certain products, services or promotions.

TRACKING TECHNOLOGIES

Cookies and Web Beacons

We may use cookies, web beacons, tracking pixels, and other tracking technologies on the Site to help customize the Site and improve your experience. When you access the Site, your personal information is not collected using tracking technology. Most browsers are set to accept cookies by default. You can remove or reject cookies but be aware that such action could affect the availability and functionality of the Site. You may not decline web beacons. However, they can be rendered ineffective by declining all cookies or by modifying your web browser's settings to notify you each time a cookie is tendered, permitting you to accept or decline cookies on an individual basis.

We may use cookies, web beacons, tracking pixels, and other tracking technologies on the Site to help customize the Site and improve your experience. For more information on how we use cookies, please refer to our Cookie Policy posted on the Site, which is incorporated into this Privacy Policy. By using the

Site, you agree to be bound by our Cookie Policy.

Internet-Based Advertising

Additionally, we may use third-party software to serve ads on the Site [and our mobile application], implement email marketing campaigns, and manage other interactive marketing initiatives. This third-party software may use cookies or similar tracking technology to help manage and optimize your online experience with us. For more information about opting-out of interest-based ads, visit the Network.

Advertising Initiative Opt-Out Tool or Digital Advertising Alliance Opt-Out Tool.

Website and Email Analytics

We may also partner with selected third-party vendors, such as Google Analytics, and others, to allow tracking technologies and remarketing services on the Site through the use of first party cookies and third-party cookies, to, among other things, analyze and track users' use of the Site to determine the popularity

of certain content and better understand online activity. By accessing the Site, you consent to the collection and use of your information by these third-party vendors. You are encouraged to review their privacy policy and contact them directly for responses to your questions. We do not transfer personal information to these third-party vendors. However, if you do not want any information to be collected and used by tracking technologies, you can visit the third-party vendor or the Network Advertising Initiative Opt-Out Tool or Digital Advertising Alliance Opt-Out Tool.

You should be aware that getting a new computer, installing a new browser, upgrading an existing browser, or erasing or otherwise altering your browser's cookies files may also clear certain opt-out cookies, plug-ins, or settings.

THIRD-PART WEBSITES

The Site may contain links to third-party websites and applications of interest, including advertisements and external services, that are not affiliated with us. Once you have used these links to leave the Site any information you provide to these third parties is not covered by this Privacy Policy, and we cannot guarantee the safety and privacy of your information. Before visiting and providing any information to any third-party websites, you should inform yourself of the privacy policies and practices (if any) of the third party responsible for that website, and should take those steps necessary to, in your discretion, protect the privacy of your information. We are not responsible for the content or privacy and security practices and policies of any third parties, including other sites, services or applications that may be linked to or from the Site.

SECURITY OF YOUR INFORMATION

We use administrative, technical, and physical security measures to help protect your personal information. While we have taken reasonable steps to secure the personal information you provide to us, please be aware that despite our efforts, no security measures are perfect or impenetrable, and no method of data transmission can be guaranteed against any interception or other type of misuse. Any information disclosed online is vulnerable to interception and misuse by unauthorized parties. Therefore, we cannot guarantee complete security if you provide personal information.

POLICY FOR CHILDREN

We do not knowingly solicit information from or market to children under the age of 13. If you become aware of any data, we have collected from children under age 13, please contact us using the contact information provided below.

CONTROLS FOR DO-NOT-TRACK FEATURES

Most web browsers and some mobile operating systems include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. No uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this Privacy Policy. Most web browsers and some mobile operating systems [and our mobile applications] include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. If you set the DNT signal on your browser, we will respond to such DNT browser signals.

OPTIONS REGARDING YOUR INFORMATION

Emails and Communications

If you no longer wish to receive correspondence, emails, or other communications from us, you may opt-out by:

- Contacting us using the contact information provided below

If you no longer wish to receive correspondence, emails, or other communications from third parties, you are responsible for contacting the third party directly.

CONTACT US

If you have questions or comments about this Privacy Policy, please contact us at:

BJK Photos, LLC

181 Kenwood Ave.

Oneida, NY 13421

(315) 280-4509

info@bjkphotos.com

Date: 9/14/2023
To: CAZENOVIA CENTRAL SCHOOL
From: BJK Photos, LLC
Re: Photography Agreement Addendum for Student Data Privacy and Security

As you know, New York enacted in the past legislative session new requirements that govern the disclosure and use of personally identifiable information of students, as well as contracts between schools and their service providers entrusted with handling such information. BJK Photos, LLC has always taken the confidentiality and security of student data and images very seriously.

In order to provide efficient delivery of school portraits to your school for distribution to students, certain basic student information is necessary. BJK Photos, LLC handles such information strictly in accordance with the conditions imposed on “school officials” by the Family Educational Rights in Privacy Act (FERPA). We have also closely monitored the progress and implementation of recent state legislative activity pertaining to student data. The purpose of this letter is to assure you that BJK Photos, LLC is fully prepared and compliant with New York Education Law Section 2-d.

To that effect, this letter, together with the attached ***FAQ for School Records Custodians***, shall serve as an Addendum to the Photography Agreement between your school and BJK Photos, LLC. These documents confirm BJK Photos, LLC commitment to meet the requirements of all applicable federal and state laws, regulations and NYSED policies, including without limitation the ***Parents Bill of Rights for Data Privacy and Security***, which is also made part of our Agreement by reference. Upon termination of the BJK Photos, LLC contract with the school district, BJK Photos, LLC will return all School Data provided to it to the school district or confirm that all provided School Data has been destroyed. No School Data will be retained by BJK Photos, LLC for longer than necessary to complete its contract with the school district.

We also want to bring to your attention that BJK Photos, LLC offers a secure portal for the transmission of student data and images to and from your school. The portal utilized by BJK Photos, LLC; PLIC Go- a product of Photolynx, was designed with student data privacy and security in mind, including the requirements set forth in New York’s Education Law § 2-d ¶5(f)(4) and 5(f)(5).

Please feel free to contact your BJK Photos, LLC account representative with any questions or concerns about this important topic.

BJK Photos, LLC

By: Elizabeth Jones
Title: Owner; President

By: Janet King
Title: Owner; VP of Operations



181 Kenwood Ave. Oneida, NY 13421
315.280.4509 info@bjkphotos.com

Important Student & Staff Data Privacy FAQ for School Record Custodians

BJK Photos, LLC is a trusted, locally owned, provider of school photography services, offering portrait photography services to schools and families in the greater Central New York region. In preparation for photo day BJK Photos, LLC requires certain directory-type information from your school to be used as follows:

- ✿ Produce and deliver portrait based products to the school for administrative purposes.
- ✿ Produce and deliver portrait based products to the school for yearbook purposes.
- ✿ Deliver Photo Day notices to families on behalf of the school.
- ✿ Provide parents the opportunity to purchase portrait products.

What Data does BJK Photos require?

The data required for photo day varies depending upon the services and deliveries the school has requested from BJK Photos. Basic class lists; including names, grade, teacher & student id numbers* are necessary before photo day to allow for perfect image and name matching and to create a photo day experience that is the least disruptive to your school and staff.

If allowed, parent email addresses are collected to allow BJK Photos to communicate directly with the parents, on the school's behalf regarding Photo Day. Information communicated is limited to photo dates, tips for preparing for photography and information about how to purchase photographs of their children.

**Student Id numbers are a requirement of most school administrative systems and allow BJK Photos to produce files for importing directly into the school's administrative systems. In addition, Student ID numbers may be required for generating Student ID cards when that service is requested.*

How does BJK Photos use the School Data?

BJK Photos, LLC uses the data only as necessary to create the school administrative products for the school and provide photography products for the families of the student. BJK Photos, LLC does not sell or license such data to others. To the extent service providers are employed by BJK Photos, LLC to assist in fulfilling BJK Photos, LLC obligations, we require strict compliance of privacy, confidentiality and security measures.

BJK Photos retains data only as necessary to promote the sale of portraits to parents and to retrieve the images to fulfill portrait orders and support the school for approved administrative purposes. Once such data is no longer required for these purposes, it is securely destroyed. While retained the images remain under BJK Photos, LLC control and is treated as confidential information.

What about FERPA?

BJK Photos, LLC acknowledges its obligations as a service provider to your school for student and staff photography pursuant to the Federal Educational Rights and Privacy Act (FERPA) and its impending regulations. As such, we affirm that BJK Photos, LLC has a legitimate need for certain School Data to provide the services to the school as contracted. Your school has the authority to control BJK Photos, LLC use of School Data including requesting the return or destruction of School Data provided to BJK Photos, LLC at any time.

In addition, BJK Photos, LLC will make every effort to meet additional data handling requirements as prescribed by state law or school district policies provided we are notified prior to disclosure.

How does BJK Photos, LLC protect School Data?

BJK Photos, LLC utilizes a variety of physical, technical and organizational measures to ensure security.

Data Center & Networks: BJK Photos, LLC data center is in complete control by authorized BJK Photos personnel. Access is limited to personnel that have the proper credentials based upon their role. Devices storing or providing access to School Data are protected with multi layer security strategies we also use to secure our own business records; including firewalls on our routers and servers, monitoring, security alerts, vulnerability scanning and authentication procedures.

Personnel: All BJK Photos, LLC employees undergo Federal and State background checks and sign a confidentiality agreement as a requirement of employment. Employees are granted access of data limited to only what is necessary to perform their job. Appropriate measures are taken to enforce these policies.

Prior to receiving access to student data and/or teacher and principal data, officer(s) and employee(s) of BJK Photos, LLC and any assignees who will have access to student data or teacher or principal data shall receive training on the federal and state laws governing confidentiality of such data. Such training shall be provided upon hire and reviewed annually.

BJK Photos, LLC is committed to child safety. We provide a complimentary Child Safety ID card for each student photographed. This card, provided to the family, includes the child's photograph and instructions as to what to do in the event their child is missing.

BJK Photos, LLC 181 Kenwood Ave. Oneida, NY 13421
315.280.4509 info@bjkphotos.com