SCHOOL PHOTOGRAPHERS OF AMERICA

Student Data Security in School Photography

What's True, What's Not, and What's Regulated

This document explains how student information is used in school photography, how information moves through systems, and what legal and operational safeguards govern the process. It is intended to provide clarity based on established practices.

1. **What student data school photography companies actually receive**
   To operate picture day accurately and efficiently, school photography companies receive a limited subset of directory-level student information provided by schools. This information is used for identification and matching purposes only, such as:

   - Ensuring each student is photographed once
   - Matching images to the correct student record
   - Delivering photo packages to the correct family
   - Allowing parents to view and order their child's photos

   This data mirrors what schools routinely share with vendors that provide yearbooks, learning platforms, transportation services, and assessment tools.

2. **What school photography companies do not receive**
   School photography companies **do not** receive sensitive or protected personal information, including but not limited to:

   - Social Security numbers
   - Medical or health records
   - Academic grades, test scores, or IEP information
   - Discipline or behavioral records
   - Immigration or citizenship status
   - Financial account or banking information
   - Parent income or employment data

This information is not required for photography services and is not part of standard Student Information System (SIS) exports for school photography purposes.

3. **How student data flows from school systems to photo fulfillment**
   The data flow process is structured, limited, and traceable.

   1. School-controlled export
      Schools generate an export from their SIS containing only the fields needed for photography. The school determines what fields are included.

   2. Secure transfer to the photography provider
      Data is transferred using secure methods such as encrypted file transfer protocols or secure vendor portals.

   3. Restricted internal access
      Within the photography company, access to student data is limited to authorized systems and personnel whose roles require it.

   4. Use limited to photography operations
      Data is used solely to support photography, ordering, and delivery. It is not repurposed or shared for unrelated uses.

   5. Defined retention and deletion
      Data is retained only as long as required to fulfill contractual obligations and is then archived or deleted according to policy.

   At each stage, access and usage can be audited.

4. **Federal laws that govern student data in school photography**

   FERPA (Family Educational Rights and Privacy Act)

   FERPA governs the disclosure and use of student education records.
   Under FERPA:

   - Schools may share limited directory information with authorized vendors acting on the school's behalf
   - Vendors may use the data only for the contracted purpose
   - Unauthorized use or disclosure is a violation of federal law

   Photography companies operate as s**chool officials with legitimate educational interest**, as defined by district contracts.

COPPA (Children's Online Privacy Protection Act)

COPPA regulates the online collection of information from children under 13.

- When photography ordering platforms are used, they operate under school consent frameworks
- Data collection is limited to what is necessary to provide the service
- Use outside of that scope is prohibited

Violations of these laws carry legal, financial, and regulatory consequences.

5. **District contracts and additional legal protections**
   Beyond federal law, school photography companies are bound by district contracts that typically include:

   - Permitted use clauses restricting data to photography services
   - Data security and confidentiality requirements
   - Data breach notification obligations
   - Data retention and destruction timelines
   - Prohibitions on resale or unrelated use of student data

   These contracts are enforceable and subject to legal review.

6. **Typical industry data security safeguards**
   Across the school photography industry, standard safeguards commonly include:
   - Role-based access controls limiting who can view student data
   - Secure login credentials and authentication requirements
   - Encrypted data transmission and storage
   - Monitoring and logging of system access
   - Vendor and subcontractor access limitations
   - Regular internal and third-party security assessments

   These safeguards are aligned with general best practices for handling limited personal data.

7. **What would be illegal or impossible under current systems**
   Under current laws, contracts, and technical structures:
   - Accessing unrelated student records would violate FERPA
   - Sharing student data outside of contracted purposes would violate district agreements
   - Mass access to sensitive student data would require school-level system breaches, not vendor access

- Undetected misuse would be technically unlikely due to access controls and audit trails

Any attempt to bypass these controls would create immediate legal and contractual exposure.

8. **Why school photography is not a unique data risk**
   School photography uses less student data than many other educational services, including:
   - Learning management systems
   - Assessment platforms
   - Transportation and food service systems
   - Communication and attendance tools

   Photography systems are purpose-limited and transactional, reducing long-term data exposure.

9. **SPOA's role**
   The School Photographers of America works to promote transparency, responsible practices, and clear understanding across the school photography industry. Our focus is education and clarity so schools and families can make informed decisions based on facts.

Closing
Student privacy is a shared responsibility. Clear understanding of how systems work helps prevent confusion, reduces unnecessary concern, and allows schools and families to focus on supporting students.

Facts, transparency, and accountability are the foundation of trust.