Book	Policy Manual
Section	Policies & Legal Updates for LAT to preview, 35-1
Title	2025 COPPA Rule - Implications for K-12 Public Schools
Code	05 - Legal Alert
Status	

Legal Alert

To: Neola Clients

From: Peters Kalail & Markakis Co., L.P.A.

Re: 2025 COPPA Rule – Implications for K-12 Public Schools

Date: August 2025

The Children's Online Privacy Protection Act ("COPPA") was enacted in 1998 to provide parents with control over the personal information collected from children under the age of thirteen (13) by websites and online services. COPPA's implementing regulations are overseen by the Federal Trade Commission ("FTC"), which is required by law to review the COPPA Rule every five (5) years. The original COPPA Rule, implemented in 2000, was last substantively amended in 2013 to reflect emerging technologies, including the increased use of mobile apps and social networking platforms by children. While the previous rules focused primarily on basic parental consent and data collection practices, the new rules are the most sweeping to date and respond to dramatic shifts in how children interact with online platforms, including the rise of artificial intelligence and biometric data use. The 2025 amendments significantly expand protections by requiring separate parental consent for third party data sharing, implementing more prescriptive security requirements, establishing data retention limits, and broadening the definition of personal information.

The 2025 Final Rule was published on April 22, 2025, and became effective on June 23, 2025, with full compliance required by April 22, 2026 (except for specific provisions pertaining to COPPA's safe harbor programs).

While COPPA primarily regulates commercial operators of websites and online services directed to children under thirteen (13), school districts are allowed to give consent to ed tech companies in lieu of parental consent as long as that data is solely used for educational purposes and not commercially. Nothing in the Final Rule alters the FTC's established guidance that permits schools to adopt educational technology without obtaining individual parental consent for each student. Nevertheless, schools must ensure that vendor platforms comply with the revised COPPA Rule and must train staff accordingly (i.e., concerning student data privacy).

KEY PROVISIONS AFFECTING K-12 SCHOOLS

- **Parental Consent and Educational Use**: Operators must now obtain verifiable parental consent before children's data (i.e., personally identifiable information ("PII")) is collected, used, or disclosed to third parties. This change is critical to ed tech vendors using third party analytics, advertising, or AI tools. Consent must be specific to each third party and disclosure purpose.
- **Definition of Personal Information**: The Final Rule contains an expanded definition of PII, which now includes biometric identifiers (e.g., fingerprints, faceprints, retina or iris scans, voiceprints), online contact information, persistent identifiers, and government-issued identifiers (e.g., Social Security Numbers, State identification numbers, birth certificates, or passport numbers). This expansion means schools and their vendors must reassess the data they collect, even passively.
- **Enhanced Transparency**: Operators are now required to provide clear, direct, written notice to parents (or schools acting as proxies) about how they plan to collect, use, and disclose children's data upon receiving consent. Specifically, the operator must identify what personal information is collected, how they intend to use it, the identities or specific categories of third parties receiving the data, the purposes for each data disclosure, and the operator's data retention and deletion practices.
- **Data Retention and Deletion**: Operators must establish and publish a written data retention policy, which places limits on how long children's data can be retained (it cannot be indefinite). Further, the Rule states that the data can be

retained only as long as is reasonably necessary to fulfill the specific purpose for which it was collected.

- **Separate Parental Consent for Third Party Disclosures**: Schools must ensure their contracts require vendors to obtain separate parental consent if any student data is disclosed beyond the school-authorized purpose.
- **Cybersecurity Requirements**: Operators must implement a written information security program that is tailored to the sensitivity of student data, including conducting annual risk assessments, and scaled to the operator's size, complexity, and nature and scope of activities. It will be important for schools to require vendors to certify compliance.
- **Clarification on Mixed Audience Sites**: Websites that attract both children and general users must implement "neutral" age gates and cannot collect any personal data until age is verified. Many K–8 tools fall into this category and must be configured accordingly.

WHAT SHOULD DISTRICTS BE DOING BETWEEN NOW AND APRIL 22, 2026?

- **Conduct a Tech Audit/Carefully Analyze Vendor Agreements**: When entering or renewing vendor contracts, schools should:
    - **Require Explicit Educational Purpose Clauses**: Ensure all contracts clearly state that student data will be used solely for educational purposes, not commercial activities or targeted advertising.
    - **Demand Data Retention Policies**: The Final Rule requires operators to obtain separate parental consent before disclosing children's personal information to any third party. The district's contracts need to specify data retention periods and deletion procedures.
    - **Verify Security Measures**: Request documentation of vendors' written security programs, including annual risk assessments and specific safeguards for children's data.
    - **Include Audit Rights**: Build in contractual rights to audit vendor compliance with COPPA requirements and data handling practices.
    - **Address Biometric Data**: For any systems collecting biometric information (facial recognition for security, fingerprint scanners), ensure specific protections and limitations are contractually defined.
    - **Indemnification Clauses**: Schools should seek to include indemnification clauses related to a vendor's non-compliance.
- **Train Staff on Updated COPPA Requirements**: Ensure staff (e.g., teachers, media specialists, and technology coordinators) understand the revised consent requirements, limitations on new platform usage, and how to identify PII under the 2025 Final Rule.
- **Update Parental Notification Practices**: Create/update template notices that explain what data is collected, which platforms are used, and how parents can opt out or view their child's data.

The FTC noted when it announced the 2025 COPPA Rule that it was coming at a critical time, as companies are increasingly trying to profit off children's data, and large ed tech companies are experiencing significant cybersecurity incidents that have led to mass breaches of sensitive student data. With these events as background, the Final new Rule seeks to strengthen parental control and impose stricter data privacy and security requirements that will directly affect K-12 operations. Proactive compliance—through staff training, contract review, and vendor oversight—is essential to safeguard student privacy and minimize institutional risk. Neola urges its client to act promptly to ensure vendor compliance by the April 22, 2026 full compliance deadline, while immediately reviewing new contracts under the enhanced standards taking effect June 23, 2025.

For further details, consult:

The Final Rule at https://www.federalregister.gov/documents/2025/04/22/2025-05904/childrens-online-privacy-protection-rule and the FTC's COPPA FAQs at https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions.

Information contained in this Legal Alert is provided for the general education and knowledge of its readers. It is not designed to be, and should not be used as, the sole source of information when analyzing and addressing a legal problem/issue, and it should not be substituted for legal advice, which relies on a specific factual analysis. Moreover, the laws of each jurisdiction are different and are constantly evolving. The information in this Legal Alert is not intended to create, and receipt of it does not constitute, an attorney-client relationship. If you have specific questions regarding a particular fact situation, you should obtain the services of competent legal counsel.