

## Embracing Technology and Sticking to the Book: Part I



December 8, 2018

**Presented by:**  
Mellissa E. Gallegos, Associate

**aa/rr**  
Atkinson, Andelson  
Loya, Ruud & Romo  
A Professional Law Corporation

Cerritos • Fresno • Irvine • Marin • Pasadena • Pleasanton • Riverside • Sacramento • San Diego

## General Overview of Legal Issues

- Contracts
- Record Retention
- California Public Rights Act
- Ownership
- Intellectual Property Rights and Obligations
- Data Security
- Pupil Records
- Title IX
- Pupil Fees
- Discipline
- Search and Seizure
- Collective Bargaining

**aa/rr**

1

## Focus For Today

- Student Data Privacy
- Contract Issues



## Student Data Privacy Laws



- **FERPA:**  
Family Education Rights and Privacy Act  
(20 U.S.C. § 1232g; 34 CFR Part 99)
- **COPPA:**  
Children's Online Privacy Protection Act  
(15 U.S.C. §§ 6501-6505)
- **CIPA:**  
Children's Internet Protection Act  
(47 U.S.C. § 254)
- **SOPIPA:**  
Student Online Personal Information Protection Act  
(Bus. & Prof. Code § 22584 et. seq.)
- **California Education Code Section 49073.1 (AB 1584)**

## FERPA

- Federal law that applies to educational institutions that receive federal funding (Public Schools, Public School Districts, and Public Colleges and Universities)
  - Purpose – To protect the privacy of student's education records
  - Subject to certain exceptions, the District must obtain consent from parents/guardians before sharing student's personally identifiable information (PII).

## COPPA

- Regulates the collection of PII for children under 13 years of age by operators of websites or online services
- Website operator must limit use of the student's PII to the education context as authorized by the District
- Website operators must not use PII for marketing or selling



## CIPA

- School districts must have an Internet Safety Policy that includes technology protection measures that block or filter Internet access to content that is:
  - Obscene;
  - Child pornography; or
  - Harmful to minors
- Internet Safety Policy must address:
  - Monitoring online activities of minors on the school district network
  - Educating minors regarding safety and security when using email, chat rooms, or other direct electronic communication
  - Unauthorized access (i.e., hacking) and other unlawful online activities by minors
  - Unauthorized disclosure, use, and dissemination of personal information

## SOPIPA – California-Specific

- SOPIPA adds to the K-12 student privacy scheme the following requirements:
  1. Operators cannot target advertise on their site, service, or application or any other site, service, or application using information acquired from students
  2. Operators cannot use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application, to create a profile for a student, except for school purposes
  3. Operators cannot sell a student's information
  4. Operators cannot disclose student information, unless for legal, regulatory, judicial, safety, or operational improvement reasons
  5. Operators must protect student information through reasonable security procedures and practices
  6. Operators must delete school - or district-controlled student information when requested by schools or districts
  7. Operators may disclose student information: when required by law; for legitimate research purposes; or for school purposes to educational agencies



## Education Code Section 49073.1



- Permits public school districts to enter into contracts with third parties for the following purposes:
  - To provide services, including cloud-based services, for the digital storage, management, and retrieval of pupil records; and
  - To provide digital educational software that authorizes a third-party provider of digital educational software to access, store, and use pupil records

## Education Code Section 49073.1 (Continued)

- All third party contracts for those technology services must contain the following terms:
  1. A statement that pupil records continue to be the property of and under the control of the school district;
  2. A description of the means by which pupils may retain possession and control of their own pupil-generated content, if applicable, including options by which a pupil may transfer pupil generated content to a personal account;
  3. A prohibition against the third party using any information in the pupil record for any purpose other than those required or specifically permitted by the contract;
  4. A description of the procedures by which a parent, legal guardian, or eligible pupil may review personally identifiable information in the pupil's records and correct erroneous information;
  5. A description of the actions the third party will take—including the designation and training of responsible individuals—to ensure the security and confidentiality of pupil records;

## Education Code Section 49073.1 (Continued)

6. A description of the procedures for notifying the affected parent, legal guardian, or eligible pupil in the event of an unauthorized disclosure of the pupil's records;
7. A certification that a pupil's records shall not be retained or available to the third party upon completion of the terms of the contract and a description of how that certification will be enforced (NOTE: This requirement does not apply to pupil-generated content if the pupil chooses to establish or maintain an account with the third party for the purpose of storing that content, either by retaining possession and control of their own pupil-generated content, or by transferring pupil-generated content to a personal account.);
8. A description of how the district and the third party will jointly ensure compliance with the federal Family Educational Rights and Privacy Act; and
9. A prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising

## Technology Contract Tips



## Vendor Agreements

### *“No One Ever Asked for that Before”*

- Institution must identify the legal and practical ramifications associated with the technology project.
  - Institutions remain liable for their data and operations even though a vendor is involved.
  - If you have to comply with laws, so does the vendor!
  - Responsibilities and risks must be allocated between the vendor and the institution.
- Some vendors may not be aware of the many legal parameters educational institutions must live with.
- Both parties must be educated about the legal issues.
  - Laws applicable to student records and personnel records
    - HIPPA, Privacy, etc.
  - Children's Internet Protection Act

## Vendor Agreements

### *“No One Ever Asked for that Before”*

- Vendor must be willing to accept responsibilities in the technology agreement.
  - Complying with litigation holds discovery requests, and/or subpoenas
  - Records retention laws and policies (i.e. Requests made under the CPRA)
  - Insurance? (Cyber risks must be identified.)

## Other Technology Contract Terms

- Ownership of Data
  - Confirm language in agreements does not transfer to vendor any rights in institution's data.
  - No data mining or use of your institution's information for vendor's business or marketing purposes.
  - Education Code section 49073.1 requires certain contracts between local educational agencies and third parties to include specified provisions about the security, use, ownership, and control of pupil records.
- Termination of Agreement
  - Who owns the data?
  - What and how will institutional data be returned (will it be in a usable format?)
  - Implementation of termination: What is your plan?

## What Do Vendors Want?

- Limit liability
- Disclaim warranties
- Incorporate terms by reference
- You to indemnify them
- Broad confidentiality



## Vendors Want You to Indemnify Them for Their Failures

- Sample Vendor Clause
  - YOU AGREE TO HOLD HARMLESS, INDEMNIFY AND, AT VENDOR'S REQUEST, DEFEND VENDOR, ITS AFFILIATES AND THEIR RESPECTIVE OFFICERS, DIRECTORS, AGENTS AND EMPLOYEES (COLLECTIVELY, "VENDOR PARTIES") FROM AND AGAINST ANY AND ALL CLAIMS (INCLUDING LIABILITIES, DAMAGES, LOSSES, COSTS AND EXPENSES AND REASONABLE ATTORNEYS' FEES) TO THE EXTENT ARISING OUT OF ANY ACTION OR PROCEEDING BROUGHT BY A THIRD PARTY AGAINST ANY ONE OR MORE OF THE VENDOR PARTIES RELATED TO THIS AGREEMENT.
  - WHAT do you think? Acceptable? Any changes?

## Vendors Want You To Indemnify Them for Their Failures

- TRANSLATION
  - YOU ARE RESPONSIBLE FOR VENDOR'S FAILURES THAT CAUSE INJURY TO OTHERS.
- SOLUTION
  - Require Vendor to indemnify your institution for data breach, breach of agreement, general negligence and IP infringement.
  - Make sure clause is not undermined by limitation of liability clause.

## Technology Contract Terms

- Scope of Work
- Payment Terms & Price
- Warranties
- Confidentiality
- Records Retention Laws and Policies
- Subpoena Response Procedures
- Public Records Act Compliance
- Intellectual Property Infringement
- Ownership of Data
- Data Backup Provisions/ Archiving
- Insurance Requirements
- Limitations on Liability
- Term
- Termination
- Definitions

## Disclaimer

This AALRR presentation is intended for informational purposes only and should not be relied upon in reaching a conclusion in a particular area of law. Applicability of the legal principles discussed may differ substantially in individual situations. Receipt of this or any other AALRR presentation/publication does not create an attorney-client relationship. The Firm is not responsible for inadvertent errors that may occur in the publishing process.



© 2018 Atkinson, Andelson, Loya, Ruud & Romo

# Thank You

For questions or comments, please contact:

{ Mellissa E. Gallegos }  
(562) 653-3200  
mgallegos@aalrr.com }

**aalrr**  
Atkinson, Andelson  
Loya, Ruud & Romo  
A Professional Law Corporation