Introduction

California school districts and County Offices of Education—collectively, Local Educational Agencies ("LEAs")—collect a vast amount of data in providing educational and related services. This data may include pupil records, medical records, financial information, and more.

With the advent of individualized learning management systems, LEAs are sharing such data with third-party vendors more than ever before. There has also been a corresponding, and sometimes competing, increase in compliance measures to protect student data. This guide is intended to provide an overview and streamline some of the key laws governing student data privacy.

Please note that the laws referenced herein may not be exhaustive. This guide contains information only and is not intended to provide legal advice, nor does it establish an attorney-client relationship. LEAs are encouraged to contact their legal counsel or member organization for any questions or clarifications concerning the content contained herein.

This guide is also available electronically at **www.f3law.com**. This guide may be updated periodically; such updates may be found in the electronic version.

This Data Privacy Guide is a collaborative project between the California Education Technology Professionals Association (CETPA), the California County Superintendents Educational Services Association (CCSESA) and Fagen Friedman & Fulfrost.

Special thanks to Gretchen M. Shipley, Partner at Fagen Friedman & Fulfrost and a member of CETPA's legal team, and Ryan Ford.

TABLE OF CONTENTS

Introduction i

The Children's Online Privacy Protection Act 1

Sample Policy Language for COPPA Compliance 3

The Children's Internet Protection Act 4

Sample CIPA-Compliant Internet Safety Policy 5

Data Privacy Requirements for Contracts with Technology Providers (California Education Code § 49073.1) 7

Sample Compliance Checklist for LEA Technology Services Agreements (California Education Code § 49073.1) 8

Sample Addendum to Technology Services Agreement for California Education Code § 49073.1 Compliance 9

Collection of Student Information from Social Media (California Education Code § 49073.6) 11

Sample Student Information Notice and Social Media Plan Pursuant to Education Code § 49073.6 12

Student Online Personal Information Protection Act ("SOPIPA") (California Business & Professions Code § 22584) 13

Family Educational Rights and Privacy Act ("FERPA") 14

Protection of Pupil Rights Amendment ("PPRA") 16

Email Retention 18

California Public Records Act 19

The Health Insurance Portability and Accountability Act ("HIPAA") 20

Privacy Impact Assessment 21

Data Breach Protocol 22

The Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act ("COPPA") is a federal law governed by the Federal Trade Commission ("FTC") that controls what information may be collected from children under the age of 13 by companies operating websites and mobile applications. (15 U.S.C. § 6501, et seq.) COPPA requires companies to post a clear privacy policy on their website or mobile application, provide notice to parents, and obtain parental consent before collecting personal information from children under the age of 13.

Under COPPA, school districts[1] are authorized to provide consent on behalf of parents and may approve a student's use of an educational program. An LEA's ability to consent on a parent's behalf is strictly limited to the educational context. That is, an LEA may only consent on the parent's behalf if the personal information collected is used strictly for educational purposes and not for any commercial purpose. Additionally, the FTC recommends that an LEA provide notice on its website identifying all of the websites and applications for which the LEA has provided consent on a student's behalf.

What is Personal Information?

For COPPA purposes, personal information is individually identifiable information collected online, including:

- A first and last name;
- A home or other physical address including street name and name of a city or town;
- Online contact information as defined in this section;
- A screen or user name where it functions in the same manner as online contact information, as defined in this section;
- A telephone number;
- A social security number;
- A persistent identifier that can be used to recognize a user over time and across different websites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol ("IP") address, a processor or device serial number, or unique device identifier;
- A photograph, video, or audio file where such file contains a child's image or voice;
- Geolocation information sufficient to identify street name and name of a city or town; or
- Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Consent to Collection of Student Data is Presumed

An LEA may act as a parent's agent and can consent to the collection of a student's information on the parent's behalf, as long as the consent is limited to the educational context. Technically, in order for a commercial website operator that collects, uses, or discloses personal information from children under 13 to get consent from the school, the operator must provide the school with

[1] COPPA specifically references school districts, but given that County Offices of Education ("COE") may utilize student data in the exact same way as California school districts, we recommend that COEs follow the same guidelines as school districts. Accordingly, LEAs are referred to generally in this section even though COPPA only specifically identifies school districts.

all the notices required under COPPA. However, as long as the operator limits use of the student's information to the educational context authorized by the LEA, the operator can presume that the LEA's authorization is based on the LEA having obtained parental consent.

Website Operators Must Provide LEA with Information Upon Request
Upon request from the LEA, website operators must provide: a description of the types of personal information collected; an opportunity to review the child's personal information and/or have the information deleted; and the opportunity to prevent further use or online collection of a child's personal information.

FTC-Recommended Best Practices

- Allow parents to review the personal information collected.
- Ensure operators delete a student's personal information once the information is no longer needed for its educational purpose.
- LEAs should make available to parents notice of the websites and online services to which it has provided consent on behalf of the parent concerning student data collection, as well as the operators' direct notices. This information or a link to this information can be maintained on the LEA website.

FTC-Recommended Inquiries
According to the FTC, in deciding whether to use online technology with students, an LEA should be careful to understand how an operator will collect, use, and disclose personal information from its students. Among the questions that LEAs should ask potential operators are:

- What types of personal information will the operator collect from students?
- How does the operator use this personal information?
- Does the operator use or share the information for commercial purposes not related to the provision of the online services requested by the LEA?
- Does the operator enable the LEA to review and have deleted the personal information collected from its students? If not, the LEA cannot consent on behalf of the parent.
- What measures does the operator take to protect the security, confidentiality, and integrity of the personal information that it collects?
- What are the operator's data retention and deletion policies for children's personal information?

Policy and Notice of Right to Opt Out of Data Collection for Marketing
LEAs must adopt policies and provide direct notification to parents at least annually regarding the rights of parents to opt their children out of participation in activities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or selling that information (or otherwise providing that information to others for such purpose).

For more information on COPPA, see Section M: COPPA and Schools on www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

Sample Policy Language for COPPA Compliance

The following sample language can be inserted into a Board Policy governing Pupil Records and/or an Acceptably Use of Technology Policy or similar:

> The District is pleased to be able to offer individualized instruction to students through a variety of technological resources. In some instances, the District will offer educational websites or applications that utilize personal information of students, such as name, screen name, user name, etc., in order to provide the individualized instruction. A list of such websites and applications and links to their terms and conditions may be found on the District website.
>
> Additionally, the District tries to avoid websites and applications that market or sell student personal information. Should such a website or application be utilized for educational purposes, it will be identified on the District website and parents have the right to opt out of student use of such websites and applications.

(Note: The foregoing COPPA requirements only apply to students under the age of 13. However, it is good practice to apply the same rules to all students throughout a school district.)

Practice pointer:

LEAs should train staff to review the terms and conditions of websites and applications to determine whether student data is collected for marketing and advertising purposes. A procedure should also be established for staff to report, for inclusion on the LEA website, which educational websites and applications collect personal information of students and where the LEA has consented on behalf of students.

The Children's Internet Protection Act

The Children's Internet Protection Act ("CIPA") is a federal law enacted to address concerns regarding children's access to obscene or harmful content over the Internet. CIPA imposes requirements on LEAs that receive discounts for Internet access or internal connections through the federal E-rate program. In order to receive E-rate funding, LEAs must certify that they have in place an Internet safety policy that includes certain technology protection measures.

Public Notice Requirement
Prior to adoption and certification of an Internet safety policy, CIPA requires sufficient public notice for at least one public meeting to address the proposed policy. A public meeting called for the purpose of complying with CIPA must be open to all.

What is Required for Certification of the Internet Safety Policy?
LEAs subject to CIPA may not receive discounts offered through the E-rate program unless they do the following:

- Certify that it has an Internet safety policy that includes protection measures that block or filter Internet access to content that is:
  - Obscene;
  - Child pornography; or
  - Harmful to minors.
- Include a provision in its Internet safety policy that requires monitoring of online activities of minors on the LEA network.
- Provide for educating minors about appropriate online behavior, including:
  - Interacting with others on social networking websites and in chat rooms; and
  - Cyberbullying awareness and response.

What Must the Internet Safety Policy Address?
The Internet safety policy must address the following six components:

- Access by minors to inappropriate matter on the Internet;
- The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communication;
- Unauthorized access, including so-called "hacking" and other unlawful activities by minors online;
- Unauthorized disclosure, use, and dissemination of personal information concerning minors; and
- Measures restricting minors' access to materials harmful to them.

Sample CIPA-Compliant Internet Safety Policy

Note: The following sample Internet safety policy was developed by E-rate Central solely to address the basic policy compliance requirements of CIPA for E-rate funding. LEAs adopting new or revised Internet policies may wish to expand or modify the sample policy language. CIPA-compliant language is typically incorporated into an LEA's Acceptable Use Policy.

Internet Safety Policy

Introduction

It is the policy of the District to: (a) prevent over its computer network user access to, or transmission of, inappropriate material via the Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act ("CIPA") [Pub. L. No. 106-554 and 47 U.S.C. § 254(h)].

Access to Inappropriate Material

To the extent practicable, technology protection measures (or "Internet filters") shall be used to block or filter access to inappropriate information over the Internet or by other forms of electronic communication.

Specifically, as required by CIPA, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage

To the extent practicable, steps shall be taken to promote the safety and security of users of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

Specifically, as required by CIPA, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Education, Supervision and Monitoring

It shall be the responsibility of all members of District staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy.

Procedures for disabling or otherwise modifying any technology protection measures shall be the responsibility of designated representatives.

The designated representatives will provide age-appropriate training for students who use the District's Internet connection. The training provided will be designed to promote the District's commitment to:

a. The standards and acceptable use of Internet services as set forth in the District's Internet safety policy;
b. Student safety with regard to:
    i. Safety on the Internet;
    ii. Appropriate behavior while online, on social networking websites, and in chat rooms; and
    iii. Cyberbullying awareness and response.
c. Compliance with the E-rate requirements of CIPA.

Following completion of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Definitions

- **Minor.** The term "minor" means any individual who has not attained the age of 17 years.
- **Technology Protection Measure.** The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:
    1. **Obscene**, as that term is defined in section 1460 of title 18, United States Code;
    2. **Child pornography**, as that term is defined in section 2256 of title 18, United States Code; or
    3. **Harmful** to minors.

- **Harmful to Minors.** The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:
    1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
    2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
    3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

- **Sexual Act; Sexual Contact.** The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

Data Privacy Requirements for Contracts with Technology Providers (California Education Code § 49073.1)

Technology services agreements entered into, amended, or renewed by an LEA on or after January 1, 2015 must follow specific requirements. These requirements apply to contracts for services that utilize electronic technology, including cloud-based services, for the digital storage, management and retrieval of pupil records, as well as educational software that authorizes a third-party provider to access, store and use pupil records. Therefore, it is recommended that any such agreements, including terms and conditions for websites and applications, be reviewed for the following terms:

- Establish that the LEA owns and controls student records.
- Describe how students can control content created for education-related purposes, along with a way to transfer content to a personal account later.
- Prohibit third parties from using student information for purposes outside of those named in the contract.
- Describe how parents, legal guardians, or students can review and correct personally identifiable information contained in their records.
- Outline actions that third parties will take to ensure student data is secure and confidential.
- Describe procedures for notifying affected parents, legal guardians, or eligible students in the event of unauthorized disclosure of student records.
- Certify that student records will not be retained or available to the third party once the contract is over and explain how that will be enforced.
- Describe how LEAs and third parties will comply with FERPA.
- Prohibit third parties from using personally identifiable information from student records to target advertising to students.

LEAs should be cautioned that out-of-state technology providers may not be familiar with these requirements. The penalty for noncompliance with the requirements of Education Code section 49073.1 is that contracts will be voided if, following the provision of notice of deficiency, they do not comply within a reasonable amount of time.

A sample checklist is included to assist LEAs in evaluating compliance. In the event that an LEA determines an agreement is not compliant with California Education Code section 49073.1, a sample technology contract addendum is also included, which LEAs may provide to technology providers to incorporate compliant procedures into existing agreements.

It is recommended that staff be trained to evaluate terms and conditions for data privacy compliance prior to downloading website content or applications for students.

Sample Compliance Checklist for LEA Technology Services Agreements (California Education Code § 49073.1)

Technology services agreements entered into, amended, or renewed by a California LEA on or after January 1, 2015 must follow specific requirements. These requirements apply to contracts for services that utilize electronic technology, including cloud-based services, for the digital storage, management and retrieval of pupil records, as well as educational software that authorizes a third-party provider to access, store and use pupil records. All of the following requirements must be included in such contracts:

- ☐ A statement that pupil records continue to be the property of and under the control of the school district;
- ☐ 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;
- ☐ 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;
- ☐ 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;
- ☐ 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;
- ☐ 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;
- ☐ 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.);
- ☐ A description of how the district and the third party will jointly ensure compliance with the federal Family Educational Rights and Privacy Act; and
- ☐ A prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising.

References: AB 1584; Cal. Educ. Code § 49073.1; 20 U.S.C. § 1232g

Sample Addendum to Technology Services Agreement for California Education Code § 49073.1 Compliance

This Addendum No. __ is entered into between _____ [insert Local Educational Agency name] ("LEA") and _____ [insert service provider name] ("Service Provider") on _____ ("Effective Date".)

WHEREAS, the LEA and the Service Provider entered into an agreement for technology services titled _____ [insert original contract title] ("Technology Services Agreement") on _____ and any addenda on _____;

WHEREAS, the LEA is a California public entity subject to all state and federal laws governing education, including but not limited to California Assembly Bill 1584 ("AB 1584"), the California Education Code, the Children's Online Privacy and Protection Act ("COPPA"), and the Family Educational Rights and Privacy Act ("FERPA");

WHEREAS, AB 1584 requires, in part, that any agreement entered into, renewed or amended after January 1, 2015 between a local education agency and a third-party service provider must include certain terms; and

WHEREAS, the LEA and the Service Provider desire to have the Technology Services Agreement and the services provided comply with AB 1584.

NOW, THEREFORE, the Parties agree as follows:

1. The terms and conditions of the Technology Services Agreement and any addenda are incorporated herein by reference.

2. The term of this Addendum shall expire on the termination date stated in the Technology Services Agreement or in any addenda to such Technology Services Agreement, whichever controls.

3. Pupil records[1] obtained by Service Provider from LEA continue to be the property of and under the control of the LEA.

4. The procedures by which pupils may retain possession and control of their own pupil-generated content are outlined as follows: [INSERT PROCEDURE][2]

[1] Pupil records include any information directly related to a pupil that is maintained by the LEA or acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other LEA employees. Pupil records does not include de-identified information (information that cannot be used to identify an individual pupil) used by the third party: (1) to improve educational products for adaptive learning purposes and for customized pupil learning; (2) to demonstrate the effectiveness of the operator's products in the marketing of those products; or (3) for the development and improvement of educational sites, services, or applications.

[2] Procedure provided will likely depend on the capability of the technology services vendor. The information will likely have to be provided by vendor to demonstrate product compliance.

5. The options by which a pupil may transfer pupil-generated content to a personal account include: [INSERT PROCEDURE]

6. Parents, legal guardians, or eligible pupils may review personally identifiable information in the pupil's records and correct erroneous information by the following protocol: [INSERT PROCEDURE]

7. Service Provider shall take actions to ensure the security and confidentiality of pupil records, including but not limited to designating and training responsible individuals on ensuring the security and confidentiality of pupil records, by the following measures: [INSERT PROCEDURE]

8. In the event of an unauthorized disclosure of a pupil's records, Service Provider shall report to an affected parent, legal guardian, or eligible pupil pursuant to the following procedure: [INSERT PROCEDURE]

9. Service Provider shall not use any information in a pupil record for any purpose other than those required or specifically permitted by the Technology Services Agreement.

10. Service Provider certifies that a pupil's records shall not be retained or available to the Service Provider upon completion of the terms of the Technology Services Agreement, except for a case where a pupil chooses to establish or maintain an account with Service Provider for the purpose of storing pupil-generated content, either by retaining possession and control of their own pupil-generated content, or by transferring pupil-generated content to a personal account. Such certification will be enforced through the following procedure: [INSERT PROCEDURE]

11. LEA agrees to work with Service Provider to ensure compliance with FERPA and the Parties will ensure compliance through the following procedure: [INSERT PROCEDURE]

IN WITNESS WHEREOF, parties execute this Agreement on the dates set forth below.

Date: _____ [Insert LEA Name]

_____

Date: _____ [Insert Service Provider Name]

_____

Collection of Student Information from Social Media (California Education Code § 49073.6)

California Education Code section 49073.6 requires that LEAs considering "a program to gather or maintain in its records any pupil information obtained from social media" first notify pupils and their parents or guardians about the proposed program, and then provide an opportunity for public comment at a regularly scheduled public meeting before adopting the program.

"Social media" means an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant messages, email, text messages, online services or accounts, or Internet website profiles or locations.

For purposes of this law, "social media" does *not* mean an electronic service or account used exclusively for educational purposes or primarily to facilitate creation of school-sponsored publications, such as a yearbook or pupil newspaper, under the direction or control of a school, teacher, or yearbook adviser.

Any LEA that adopts a program pursuant to this provision must:

- Gather and maintain only information pertaining directly to school or student safety;
- Provide a student with access to any information about the student obtained from social media; and
- Destroy the information gathered from social media and maintained in its records within one year of the student turning 18 or discontinuing attendance with the LEA, whichever is sooner.

If an LEA contracts with a third party to gather student information from social media, California Education Code section 49073.6:

- Prohibits the third party from using the information for purposes other than to satisfy the terms of the contract;
- Prohibits the third party from selling or sharing the information with outside persons or entities; and
- Provides additional restrictions on the destruction of the information by the third party.

The foregoing requirements could be incorporated by an agreement with the third party.

California Education Code section 49073.6 does not specifically define "a program to gather or maintain in its records any pupil information obtained from social media." However, many LEAs research public social media sites following a complaint of cyberbullying or school-related misconduct. To the extent this information is collected, maintained, or utilized for disciplinary purposes, this practice likely falls under the definition of "a program to gather or maintain in its records any pupil information obtained from social media" and would need to meet the requirements of 49073.6.

It is recommended that the notification be simple and straightforward, emphasizing the public safety purpose behind the practice.

Sample Student Information Notice and Social Media Plan Pursuant to Education Code § 49073.6

Student Information and Social Media Notice

Anytime a school district considers a plan to gather pupil information obtained from social media, it is supposed to notify students and parents about the proposed program and provide the opportunity for public comment prior to adoption of the program.

While the District does not intend to make a practice of reviewing student social media accounts, from time to time the District may be required to investigate online content in response to a report of cyberbullying, threats, or other misconduct, in an effort to ensure a safe learning environment. Student safety is the District's top priority and we welcome the opportunity to further discuss bullying prevention, the school safety plan, or any other related issues to District investigation strategies at the _____, 20___ Board meeting.

Adoption of Plan Related to Student Information and Social Media

Designated District staff are granted the authority to conduct a reasonable investigation into alleged student misconduct, including an Internet search of public content, which includes social media sites, as defined in California Education Code section 49073.6, for evidence of such misconduct. The purpose of such an investigation would be to protect the safety of District students.

Any District staff member who has not been designated with this authority should refrain from collecting or maintaining in student records any information collected from student social media pages without first seeking approval from a District administrator and following proper procedures, including student/parent notification, and well as a public hearing prior to conducting such a program.

Student Online Personal Information Protection Act ("SOPIPA") (California Business & Professions Code § 22584)

California Business and Professions Code section 22584, also known as the Student Online Personal Information Protection Act ("SOPIPA"), takes effect on January 1, 2016 and sets forth privacy laws for operators of websites, online services, and applications that are marketed and used for K-12 school purposes, even if those operators do not contract with educational agencies. While primary responsibility for compliance with SOPIPA lies with website operators, LEAs should proceed with reasonable due diligence when evaluating technology service providers, especially providers based outside of California, to ensure their policies and procedures comply with SOPIPA.

SOPIPA adds to the K-12 student privacy scheme the following requirements:

- Operators cannot target advertising on their website or any other website using information acquired from students.
- Operators cannot create a profile for a student, except for school purposes.
- Operators cannot sell a student's information.
- Operators cannot disclose student information, unless for legal, regulatory, judicial, safety, or operational improvement reasons.
- Operators must protect student information through reasonable security procedures and practices.
- Operators must delete school- or district-controlled student information when requested by schools or districts.
- Operators must disclose student information: when required by law; for legitimate research purposes; or for school purposes to educational agencies.

Note that these are general descriptions of SOPIPA's requirements, and exceptions may apply. Please consult with your legal counsel about the application of SOPIPA in any particular situation.

Family Educational Rights and Privacy Act ("FERPA")

The Family Educational Rights and Privacy Act ("FERPA") (20 U.S.C. § 1232g; 34 C.F.R. Part 99) is a Federal law that protects the privacy of student education records. The law applies to all entities that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students." Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Parents or eligible students also have the right to request that a school correct records which they believe to be inaccurate or misleading.

Generally, LEAs must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows LEAs to disclose those records, without consent, to the following parties or under the following conditions (34 C.F.R. § 99.31):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific state law.

Directory Information

LEAs may also disclose, without consent, "directory information." FERPA defines directory information as information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. (34 C.F.R. § 99.3.) Directory information may include a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. Education records that have been appropriately designated as "directory information" by the educational agency or institution may be disclosed without prior consent. (*See* 34 C.F.R. §§ 99.31(a)(11) and 99.37.)

FERPA provides that a school may disclose directory information if it has given public notice of the types of information that it has designated as "directory information," the parent or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information." (34 C.F.R. § 99.37(a).)

Therefore, many school districts include in their annual FERPA notice a broad designation of what is considered directory information and the circumstances of when it can be released without parental consent. Again, this notice should also give parents and eligible students the opportunity to restrict such disclosure.

Disclosure to "School Officials"
Another exception, which permits disclosure without consent, is disclosure to school officials with a legitimate educational interest in the information. LEAs must include in their annual FERPA notice, how they define "school official" and "legitimate educational interest."

A "school official" is a person employed by the school as an administrator, supervisor, instructor, or support staff member (including health or medical staff and law enforcement unit personnel) or a person serving on the school board. A school official also may include a volunteer or contractor outside of the school who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of personally identifiable information from education records, such as an attorney, auditor, medical consultant, or therapist; a parent or student volunteering to serve on an official committee, such as a disciplinary or grievance committee; or a parent, student, or other volunteer assisting another school official in performing his or her tasks.

A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility. LEAs sometimes disclose educational records to technology vendors under the "school official" exception when the vendor is performing an institutional service or function of the LEA and the records are required to fulfill this function.

Technology vendors often qualify as a "school official" for purposes of the exemption to the Public Records Act, which allows directory information to be shared to a third-party application or website.

Protection of Pupil Rights Amendment ("PPRA")

PPRA is a federal law that applies to the programs and activities of a state educational agency ("SEA"), local educational agency ("LEA"), or other recipient of funds under any program funded by the U.S. Department of Education. It governs the administration to students of a survey, analysis, or evaluation that concerns one or more of the following eight protected areas:

1. Political affiliations or beliefs of the student or the student's parent;
2. Mental or psychological problems of the student or the student's family;
3. Sex behavior or attitudes;
4. Illegal, anti-social, self-incriminating, or demeaning behavior;
5. Critical appraisals of other individuals with whom respondents have close family relationships;
6. Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers;
7. Religious practices, affiliations, or beliefs of the student or student's parent; or,
8. Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

PPRA also concerns marketing surveys and other areas of student privacy, parental access to information, and the administration of certain physical examinations to minors. The rights under PPRA transfer from the parents to a student who is 18 years old or an emancipated minor under state law.

LEAs must provide parents and eligible students effective notice of their rights under PPRA. The notice must explain that an LEA is required to obtain prior written consent from parents before students are required to submit to a survey that concerns one or more of the eight protected areas listed above, if the survey is funded in whole or in part by Department funds. For surveys that contain questions from one or more of the eight protected areas that are not funded in whole or in part with Department funds, LEAs must notify a parent at least annually, at the beginning of the school year, of the specific or approximate date(s) of the survey and provide the parent with an opportunity to opt his or her child out of participating. LEAs must also notify parents that they have the right to review, upon request, any instructional materials used in connection with any survey that concerns one or more of the eight protected areas and those used as part of the educational curriculum.

PPRA requires LEAs to work with parents to develop and adopt policies on the following items, unless the LEA or SEA had established comparable policies on or before January 8, 2002:

- The right of parents to inspect, upon request, a survey created by a third party before the survey is administered or distributed by a school to students and the procedure for granting a request by a parent for such access;
- Arrangements to protect student privacy that are provided by the LEA in the event of the administration of a survey to students containing one or more of the eight protected items of information noted above (including the right of parents to inspect, upon request, a survey that concerns one or more of the eight protected items of information);

- The right of parents to inspect, upon request, any instructional material used as part of the educational curriculum for students, and the procedure for granting a request by a parent for such access;
- Administration of physical exams or screenings of students;
- The collection, disclosure, or use of personal information (including items such as a student's or parent's first and last name, address, telephone number or social security number) collected from students for marketing purposes, or to sell or otherwise provide the information to others for marketing purposes, including the LEA's arrangements for protecting student privacy in the event of collection, disclosure, or use of information for these purposes; and
- The right of parents to inspect, upon request, any instrument used in the collection of personal information for marketing or sales purposes before the instrument is administered or distributed to a student and the LEA's procedure for granting a parent's request for such access.

LEAs must notify parents of their rights under PPRA and of these policies at least annually at the beginning of the school year. LEAs must also notify parents within a reasonable period of time if any substantive change is made to the policies. (This notification requirement may be included in the general notification of rights under PPRA.) An LEA is not required to develop and adopt new policies if the SEA or LEA had in place on January 8, 2002, policies covering the requirements set forth in this law. However, the LEA must still provide annual notice of these policies to parents.

PPRA does not preempt applicable provisions of state law that require parental notification. Also, requirements concerning activities involving collection and disclosure of students' personal information for marketing purposes do not apply to the collection, disclosure, or use of personal student information collected for the exclusive purpose of developing, evaluating, or providing educational products or services for or to students or educational institutions, such as the following:

- College or other postsecondary education recruitment, or military recruitment;
- Book clubs, magazines, and programs providing access to low-cost literary products;
- Curriculum and instructional materials used by elementary schools and secondary schools;
- Tests and assessments used by elementary schools and secondary schools to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students (or to generate other statistically useful data for the purpose of securing such tests and assessments) and the subsequent analysis and public release of the aggregate data from such tests and assessments;
- The sale by students of products or services to raise funds for school-related or education-related activities; and
- Student recognition programs.

Under the PPRA, "personal information" is defined as individually identifiable information including:

- A student's or parent's first and last name;
- A home or other physical address (including a street name and name of a city or town);
- A telephone number; or
- A social security number.

Email Retention

Many LEA servers are clogged with emails that never get deleted for fear they will be destroyed prior to any applicable mandatory retention period. LEAs may want to establish a procedure for staff to determine whether and for how long an email must be retained, as well as a process for forwarding emails for data storage.

When Is an Email a "Record" for Purposes of Record Retention?
It is the content of a record, not its medium, that determines whether it must be retained and for how long. For purposes of classification to determine the retention period, records are defined as "maps, books, papers, and documents of a school district required by law to be prepared or retained or which are prepared or retained as necessary or convenient to the discharge of official duty." (5 C.C.R. § 16020.)

Thus, electronic "documents" such as emails could be considered records if the LEA is required to prepare or retain them pursuant to law or official duty. Otherwise, an email is not considered a record subject to classification and retention.

What Is the Applicable Retention Period of an Email That Qualifies as a "Record"?
The California Department of Education ("CDE") requires that LEAs classify records as either permanent, temporary, or disposable. Detailed definitions for each of these types of classifications can be found in the California Code of Regulations in Title 5, section 16023, et seq.

In addition to the permanent, temporary, and disposable classifications set forth by CDE, there are several state and federal laws that govern how long an employer, including an LEA, must retain records. These retention periods range from 1 to 6 years, or in some cases until an administrative claim has been completed or a statute of limitations period has run. Most LEAs have policies outlining these record retention periods.

If an LEA anticipates litigation or is involved in active litigation, it is recommend that it consult with legal counsel before any emails related to that matter are deleted. This may also be referred to as a "litigation hold."

Email Retention Policy
An email retention policy should, at the very least, include language that distinguishes between emails that *must* be retained and emails that *may* be deleted because they are not "records." For example, a policy could state: "Unless classified as a record that must be retained by law, email correspondence is generally not a 'record' and will not be retained by the District." Of course, an LEA may wish to retain general emails, even if not considered "records," for a longer period.

California Public Records Act

The purpose of the California Public Records Act ("PRA") is to provide the public with access to information in the possession of public agencies. The general rule is that all public records are subject to disclosure unless the legislature has expressly provided to the contrary.

Public Record Defined
Public records include any writing containing information relating to the conduct of the public's business that is prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. If part of the record is exempt, the agency is required to produce the segregable portion of the record.

Request for Public Records
Requests for public records must be reasonably focused and specific. The public agency is obligated to assist the requesting party in framing the request if the initial request is misguided. An agency is obliged to comply with a request under the PRA so long as the record can be located with reasonable effort and the request does not fall within one of the many exceptions to the PRA.

The Following Categories of Records May Be Exempt From Disclosure:

- Preliminary drafts, notes, or interagency or intra-agency memoranda that are not retained by the public agency in the ordinary course of business, if the public interest in withholding those records clearly outweighs the public interest in disclosure.
- The home addresses and telephone numbers of state employees and employees of LEAs, subject to specific statutory exceptions.
- Other than individual examinations issued to a pupil and scored, test questions or materials that would be used to administer an examination and are provided by the State Department of Education and administered as part of a statewide testing program of pupils enrolled in the public schools, upon the request of any member of the legislature or upon request of the Governor or his or her designee.
- Security record of a public agency that would reveal vulnerabilities in its information technology systems.
- Electronically collected personal information received, collected, or compiled by a state agency.

Timeline to Produce Records
An agency has 10 days to decide if copies will be provided. In "unusual" cases (request is "voluminous," seeks records held off-site, or requires consultation with other agencies), the agency may upon written notice to the requestors give itself an additional 14 days to respond. These time periods may not be used solely to delay access to the records.

The Health Insurance Portability and Accountability Act ("HIPAA")

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a comprehensive federal law that addresses a number of health care-related topics in the United States Code.

Who Does HIPAA Apply to?
HIPAA applies to health information created or maintained by "health care providers" who engage in certain electronic transactions, as well as applying to health plans and health care clearinghouses. A school may subjects itself to HIPAA if the school employs a health care provider, such as a school nurse, who engages in a HIPAA protected electronic transaction.

What Information Is Protected Under HIPAA?
HIPAA covers protected health information ("PHI"), which is individually identifiable health information transmitted or maintained in any form. PHI is information that identifies the individual or information that can be used to identify an individual. Information is covered in any form when it is created or received by a health care provider, employer, health plan, health care clearinghouse, school or university.

What Records Are *Not* Subject to HIPAA?
Records protected under FERPA are not subject to HIPAA. The scope of the HIPAA privacy rules were limited in this way to avoid unnecessary duplications.

Examples of School-Related Data Protected by HIPAA:

- A school-based health clinic operated by an outside entity, which handles billing and maintenance of records; and

- Electronic filing of Medicaid claims.

Examples of School-Related Data *Not* Subject to HIPAA:

- Student health records are typically protected by FERPA and not subject to HIPAA; and

- Health related records connected to an Individualized Education Plan ("IEP") are also usually protected by FERPA and not subject to HIPAA.

Privacy Impact Assessment

LEAs may want to conduct a Privacy Impact Assessment ("PIA") when considering the acquisition of new technology that will collect and/or utilize student data. The U.S. Department of Justice currently requires all federal agencies to conduct an extensive PIA for all federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form.

A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. Subject to certain exceptions, federal agencies are required to make PIAs publicly available.

While PIAs are not yet required for LEAs, such an analysis may be helpful to LEAs to demonstrate that any new technology is thoroughly vetted and privacy implications have been adequately considered, especially if the technology at issue is controversial or collecting highly sensitive data.

For more information regarding the components of a PIA, see http://www.justice.gov/opcl/privacy-compliance-process. Again, since PIAs are not required of LEAs, a more streamlined analysis may be appropriate under the circumstances.

Data Breach Protocol

LEAs that own computerized data that include personal information are required to disclose any breach of their security systems in an expedited manner. (*See* Cal. Civ. Code § 1798.29; *see also* Cal. Gov. Code § 6252.)

What Is a Breach?
A breach of a security system means "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency." (Cal. Civ. Code § 1798.29(e).)

What Is Personal Information? Unencrypted information containing:

- Individuals' names or initials;
- Social security numbers;
- California driver's license number or identification numbers;
- Financial information (i.e., bank account number, credit or debit card number);
- Medical information; or
- Health insurance information.
  (Cal. Civ. Code § 1798.29.)

When Must Notice of Breach Be Provided?
The law requires that notification be provided in an expedited manner upon discovering the breach. While not specifically defined in the law, notice should be provided as soon as reasonably possible. Please note that the notice may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. (Cal. Civ. Code § 1798.29(c).)

To Whom Must Notice of Breach Be Provided?
To Those Impacted. Notice of breach must be provided to those impacted by the breach. (Cal. Civ. Code § 1798.29.)

To the Attorney General, if 500+ People Impacted. If the data breach involved more than 500 individuals' personal information, and the LEA determines that it is required to provide notice of the breach to more than 500 California residents, then the LEA must also electronically provide a copy of the notice to the Attorney General's office. (Cal. Civ. Code § 1798.29(f).)

To Employees. If an employee was logged into the device at the time of the breach, the LEA should inform the employee(s) to change their passwords, security questions or answers, or other confidential information if that information was contained in that device. (*See* Cal. Civ. Code § 1798.29(c).)

What Information Must the Notice Contain?
The notice must be written in plain English, be dated, and at a minimum, include the following:

1. The name and contact information of the LEA;
2. The type of personal information that the LEA reasonably believed was obtained as a result of the breach;
3. If known, the date or estimated date of the breach;

4. Whether the notification of the breach was delayed as a result of law enforcement, if applicable;
5. A general description of the breach incident; and
6. The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed social security numbers, driver's licenses, or identification card numbers.
   (Cal. Civ. Code § 1798.29(d).)

The Notice *May* Also Include:
What the agency has done to protect individuals whose information has been breached, and advice on steps the person whose information has been breached may take to protect himself or herself. (Cal. Civ. Code § 1798.29(d).)

Can the Notice Be Sent Via Email?
The notice may be provided in electronic form only if the individual:

- Consented to receiving the electronic communication subject matter in a manner that reasonably demonstrates he or she may access the electronic communication;
- Has not withdrawn consent to receiving that electronic communication;
- Had been notified of his or her right to receive and/or request written communication;
- Had been notified of his or her right to withdraw consent to receipt of the electronic communication and the consequences of the withdrawal; and
- Was provided with a statement of the hardware and software requirements for access to electronic communication.
  (Cal. Civ. Code § 1798.29(i); *see also* 15 U.S.C. § 7001.)

In the LEA context, it is unlikely that all of the foregoing conditions will have been met to warrant that notice of a data breach be provided via email only.

Can Substitute Notice Be Provided?
The agency may also provide substitute notice if it determines that the cost of providing notice would exceed $250,000, the impacted individuals exceeds 500,000, or the agency does not have sufficient contact information. (Cal. Civ. Code § 1798.29(i).) Substitute notice must satisfy all of the following:

- Email notice when the agency has an email address for the impacted individuals;
- Conspicuous posting of the notice on the agency's website; and
- Notification to major statewide media and the Office of Information Security within the Department of Technology.
  (Cal. Civ. Code § 1798.29(i).)

Like email notification, in the LEA context, it is unlikely the foregoing conditions will have been met to warrant substitute service.