Student Data Privacy Guidelines

Student data collection is restricted to legitimate educational use.

Version as of May 4, 2016

TABLE OF CONTENTS

STUDENT DATA PRIVACY GUIDELINES

BACKGROUND

Students have a right to data privacy.

Districts need to comply with the Family Educational Rights and Privacy Act of 1974 (FERPA), as amended (20 U.S.C. § 1232g; 34 CFR Part 99), the California Information Practices Act (California Civil Code Section 1798 et seq.), California Education Code Section 49062 et seq., Student Online Personal Information Protection Act (SOPIPA), California Education Code 49073.6, California Education Code 49073.1, Article 1, Section 1 of the California Constitution, and all other applicable federal and state laws and regulations that safeguard education records, privacy, and confidentiality.

GOAL

Now, perhaps more than ever before, districts must define their own legitimate uses for student data and develop policies to manage them[1]. Schools are increasingly using educational technology ("edtech") and other cloud-based services. While this technology presents potential advantages in promoting and evaluating personalized learning, it also significantly raises the probability of student information breaches and of student privacy abuse while increasing the potential liability of the district.

> Note that **[bracketed bold red]** comments in these guidelines may be addressed by each district individually for inclusion or modification within its Board policies.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) AND OTHER FEDERAL LAWS

Federal laws safeguarding the confidentiality of student information and data privacy are contained in four main laws:

1. The Family Educational Rights and Privacy Act (FERPA, 1974) is the primary legislation that sets parameters on accessibility and disclosure of student records.
2. The Grassley Amendment (1994) to the Goals 2000: Educate America Act of 1994 details privacy of student participation in surveys, analyses, and evaluations.

[1] Policies should govern what student information is collected, the modes and methods for storage and security of the student information collected, rules for access to the student information (i.e., who can see this student information as well as what information can be shared with colleges to which students apply as well as other organizations or individuals), and rules for retention of the student information (i.e., how long this student information should be kept).

3. The Drug Abuse Office and Treatment Act (1976) protects drug and alcohol treatment records of students kept by any institution receiving federal assistance.
4. The Individuals with Disabilities Education Act (IDEA, 1997), in addition to the above acts, affects records of students in special education.

These four acts provide a structure for laws concerning confidentiality and its application as a safeguard for students and professionals. These laws specify certain requirements and obligations of participating agencies, including local educational agencies (LEA), in the control and disbursement of records and provide parents and students rights to access these records.

FERPA

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

This act, also known as the Buckley Amendment, was enacted by Congress in 1974 to guarantee parents and students a certain degree of confidentiality and fundamental fairness with respect to the maintenance and use of student records. 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. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.

Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

Generally, schools 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 schools to disclose those records, without consent, under certain conditions (34 CFR § 99.31). (See **SAMPLE DISTRICT POLICY – DATA PRIVACY 1**)

Critics complained that this law, written for when student records were mainly kept on paper, has not kept pace with digital techniques, such as data-mining. Privacy advocates have explained that many details now collected by education sites and apps were not covered by FERPA because they do not form part of the institutional student education records maintained by schools. In September 2014, California significantly extended privacy protections afforded to students' education records with SOPIPA, Education Code 49073.6, and Education Code 49073.1.

Grassley Amendment

The Grassley Amendment (1994) replaced and modified the Hatch Amendment to the General Education Provisions Act. It expanded language to the Hatch Amendment which protects pupil rights in conjunction with any survey, analysis, or evaluation of any applicable program within the school setting. This amendment applies to all programs where federal money is involved in the implementation or maintenance of the program. It also grants individuals the right to inspect materials (e.g. manuals, tapes, films) used in connection with any survey, analysis, or evaluation. Written consent of parents or eligible students must be secured by districts for the above activities before information is collected that reveals:

- Political affiliations
- Mental or psychological problems
- Sexual behavior or attitudes
- Illegal, anti-social, self-incriminating, and demeaning behavior
- Critical appraisals of other individuals with whom the students have a close family relationship
- Legally recognized privileged or analogous relationships, such as those of physicians, lawyers, or ministers, and/or
- Income, except for that information required to determine eligibility for financial assistance

The statute does not apply to information gathering that is entirely voluntary. Difficulties exist as a result of the Grassley Amendment (FERPA, 1974). First, although it requires written consent from parents, the words "informed consent" do not appear in the law. This

may create difficulties as parents may give consent without being truly informed nor fully understanding the consent they are providing to the school or researcher. Additionally, on June 6, 1991, the U.S. Department of Education revised federal regulations concerning research with human beings and experimental procedures used in public schools to develop new instructional methods. Curricula or classroom management techniques are exempt from the regulations.[2]

Drug Abuse Office and Treatment Act

Confidentiality of records of persons receiving drug or alcohol abuse treatment is protected under federal law (Drug Abuse Office and Treatment Act, 1976). This law applies to any program assisted in any way by the federal government. These requirements apply to all records relating to the identity, diagnosis, prognosis, or treatment of any student involved in any federally assisted substance abuse program. All records must be maintained in a locked and secured area. Since these regulations are generally stricter, treatment records should be maintained separately from other educational records. Records, generally, may not be disclosed without written consent of the student. Under applicable state law, minor clients with legal capacity must give consent for any release of information, including to the minor's parents. If state law requires parental consent to obtain treatment, then both parent and student must give consent before disclosure of information. Three disclosures may be made without consent:

- To medical personnel in the case of a bona fide medical emergency
- To qualified personnel conducting scientific research or audits without individual identities disclosed
- To any person with an appropriate court order

Treatment records cannot be used to conduct a criminal investigation or substantiate criminal charges against a person.

IDEA

The Individuals with Disabilities Education Act (1997) requires procedures to provide a free and appropriate public education (FAPE) for all children with disabilities. Inherent within FAPE are safeguards prohibiting the disclosure of any personally identifiable information.

Clear guidelines have been set forth for public schools when collecting, storing, releasing,

[2] See http://www.hhs.gov/ohrp/regulations-and-policy/regulations/45-cfr-46/index.html#46.401

or destroying students' personally identifiable information. These guidelines are set forth in federal legislation and state educational plans and include any participating agency that collects, maintains, or uses personally identifiable information.

Under laws governing confidentiality, participating agencies must have written procedures in the primary language of the parents that notify parents of their right to inspect records and of how information is stored, disclosed, retained, and destroyed. In addition, annual notice must be given to parents on their right to file a complaint or amend their child's records.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

Student data privacy concerns often trigger HIPAA data privacy concerns because districts collect and use student health data. In most cases, HIPAA Privacy Rules do not apply to K-12 schools because schools either (1) are not HIPAA covered entities or (2) are HIPAA covered entities but maintain health information only on students in records that are by definition "education records" under FERPA and, therefore, are not subject to the HIPAA Privacy Rule.

In the first case, a school is not a HIPAA covered entity. The HIPAA Privacy Rule only applies to health plans, health care clearinghouses, and those health care providers that transmit health information electronically in connection with certain administrative and financial transactions ("covered transactions"). (See 45 CFR § 160.102) Covered transactions are those for which the U.S. Department of Health and Human Services has adopted a standard, such as health care claims submitted to a health plan. (See the definition of "transaction" at 45 CFR § 160.103 and 45 CFR Part 162, Subparts K–R.) Thus, even though a school employs school nurses, physicians, psychologists, or other health care providers, a school is not generally a HIPAA covered entity because the providers do not engage in any of the covered transactions, such as billing a health plan electronically for their services. It is expected that most elementary and secondary schools fall into this category.

In the second case, the school is a HIPAA covered entity but does not have "protected health information." Where a school does employ a health care provider that conducts one or more covered transactions electronically, such as electronically transmitting health care claims to a health plan for payment, the school is a HIPAA covered entity and must comply with the HIPAA Transactions and Code Sets and Identifier Rules with respect to such transactions. However, even in this case, many schools would not be required to comply with the HIPAA Privacy Rule because the school maintains health information only

in student health records that are "education records" under FERPA and, thus, not "protected health information" under HIPAA. Because student health information in education records is protected by FERPA, the HIPAA Privacy Rule excludes such information from its coverage. (See the exception at paragraph (2)(i) to the definition of "protected health information" in the HIPAA Privacy Rule at 45 CFR § 160.103.) For example, if a public high school employs a health care provider that bills Medicaid electronically for services provided to a student under the IDEA, the school is a HIPAA covered entity and would be subject to the HIPAA requirements concerning transactions. However, if the school's provider maintains health information only in what are education records under FERPA, the school is not required to comply with the HIPAA Privacy Rule. Rather, the school would have to comply with FERPA's privacy requirements with respect to its education records, including the requirement to obtain parental consent (34 CFR § 99.30) in order to disclose to Medicaid billing information about a service provided to a student.

STUDENT ONLINE PERSONAL INFORMATION PROTECTION ACT (SOPIPA)

Effective January 1, 2016, the Student Online Personal Information Protection Act (SOPIPA) (Business and Professions Code Section 22584) prohibits an operator of an internet website, online service, online application, or mobile application that is used, designed, and marketed primarily for K-12 school purposes from (1) knowingly engaging in targeted advertising to students or their parents or guardians on the site, service, or application, (2) engaging in targeted advertising on a different site, service, or application using any information that was acquired from the operator's site, service or application, (3) using information created or gathered by the operator's site, service, or application to generate a profile about a student, (4) selling a student's information, and (5) disclosing certain information pertaining to a student. The law also requires the operator to maintain reasonable security measures to protect the student's information from unauthorized access, destruction, use, modification, or disclosure.

SOPIPA, *prohibits operators of online educational services from selling student data and using such information to target advertising to students or to "amass a profile" on students for a non-educational purpose. The law also requires online service providers to maintain adequate security procedures and to delete student information at the request of*

PROTECTION OF STUDENTS' SOCIAL MEDIA INFORMATION

Education Code 49073.6 (Assembly Bill 1442) currently

regulates the use of students' social media information. If a school intends to implement a program to gather students' social media information, the school must notify students and parents or guardians about the proposed program and provide an opportunity for public comment. If the program is adopted, the school must only gather or maintain information that pertains directly to school or student safety. Furthermore, the school must provide the student with access to his or her information and an opportunity to correct or delete such information, destroy information after the student turns 18 or is no longer enrolled at the school, and notify each parent or guardian that the student's social media information is being collected.

It is important to note that the law also imposes requirements on third parties that are retained by schools to gather the social media information of students. Under the law, a third party may not use the information for any purpose other than to satisfy the contract, may not sell or share the information, and must destroy the information immediately upon conclusion of the contract.

PROTECTION OF STUDENTS' RECORDS IN DIGITAL STORAGE SERVICES

Effective January 1, 2015, Assembly Bill 1584 (Education Code 49073.1) permits a school to use a third party for the digital storage, management, and retrieval of student records, or to provide digital educational software or both. In order to protect those records, any such contract with a third party must contain certain provisions, including a statement that all of the records remain the property of and under the control of the school, a description of the procedures that will be used to notify affected students, parents or guardians in the event of any unauthorized disclosure, a prohibition against using students' information for any purposes other than those required by the contract, and a certification that students' information will not be available to the third party upon completion of the contract.

"Outside a typical American middle school, papers were blowing around in the wind beside a garbage container. A student, seeing the papers, grabbed some and read about the special needs assessment for a seventh-grader named Kevin, including his IQ score, psychological assessment data, behavioral information, and family history. Some time later, the prying student and his friends were passing Kevin's private information around the school. It doesn't take a career educator to guess what happened next: Over the next few weeks, students relentlessly taunted Kevin, calling him "stupid," "dumb," and "retarded." They might just as well have applied the first of those adjectives to their school. In one careless stroke, the school's poor data security practices had led to the direct harm of one of its students.

Unfortunately, this cautionary tale isn't apocryphal. Part of a very real case out of Minnesota, it not only points out the ethical need to secure student data, but highlights the legal implications of failing to do so. Kevin's family sued the school district, and at the trial court, the jury returned a verdict that found the district liable for $60,000 in past damages and $80,000 in future damages--and also awarded more than $45,000 in legal fees to the family (although the legal fees were later reduced on appeal)."

From "How Little Data Breaches Cause Big Problems For Schools,"
T.H.E. Journal, By Justin Bathon, 11/05/2013

SAMPLE DISTRICT POLICY – DATA PRIVACY 1

Model Notification of Rights under FERPA for Elementary and Secondary Schools

The Family Educational Rights and Privacy Act (FERPA) affords parents and students, who are 18 years of age or older ("eligible students"), certain rights with respect to the student's education records. These rights are:

1. The right to inspect and review the student's education records within 45 days after the day the **[Name of school ("School")]** receives a request for access.
   Parents or eligible students should submit to the school principal **[or appropriate school official]** *a written request that identifies the records they wish to inspect. The school official will make arrangements for access and notify the parent or eligible student of the time and place where the records may be inspected.*
2. The right to request the amendment of the student's education records that the parent or eligible student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.
   Parents or eligible students who wish to ask the **[School]** *to amend a record should write the school principal* **[or appropriate school official],** *clearly identify the part of the record they want changed, and specify why it should be changed. If the school decides not to amend the record as requested by the parent or eligible student, the school will notify the parent or eligible student of the decision and of their right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the parent or eligible student when notified of the right to a hearing.*
3. The right to provide written consent before the school discloses personally identifiable information (PII) from the student's education records, except to the extent that FERPA authorizes disclosure without consent.
   One exception, which permits disclosure without consent, is disclosure to school officials with legitimate educational interests. 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 or 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 PII 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.
   [[Optional] Upon request, the school (may or will?) disclose education records without consent to officials of another school district in which a student seeks or intends to enroll or is already enrolled if the disclosure is for purposes of the student's enrollment or transfer.] [NOTE: FERPA requires a school district to make a reasonable attempt to notify the parent or student of the records request unless it states in its annual notification that it intends to forward records on request.]
4. The right to file a complaint with the U.S. Department of Education concerning alleged failures by the **[School]** to comply with the requirements of FERPA. The name and address of the office that administers FERPA are:

   Family Policy Compliance Office
   U.S. Department of Education
   400 Maryland Avenue, SW

Washington, DC 20202

[NOTE: In addition, a school may want to include its directory information public notice, as required by §99.37 of the regulations, with its annual notification of rights under FERPA.]

[Optional] See the list below of the disclosures that elementary and secondary schools may make without consent.

FERPA permits the disclosure of PII from students' education records, without consent of the parent or eligible student, if the disclosure meets certain conditions found in §99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the parent or eligible student, §99.32 of the FERPA regulations requires the school to record the disclosure. Parents and eligible students have a right to inspect and review the record of disclosures. A school may disclose PII from the education records of a student without obtaining prior written consent of the parents or the eligible student:

- To other school officials, including teachers, within the educational agency or institution whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in §99.31(a)(1)(i)(B)(1) - (a)(1)(i)(B)(2) are met. (§99.31(a)(1))
- To officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of §99.34. (§99.31(a)(2))
- To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as the state educational agency in the parent or eligible student's state (SEA). Disclosures under this provision may be made, subject to the requirements of §99.35, in connection with an audit or evaluation of federal- or state-supported education programs, or for the enforcement of or compliance with federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35)
- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4))
- To state and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a state statute that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records were released, subject to §99.38. (§99.31(a)(5))
- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§99.31(a)(6))
- To accrediting organizations to carry out their accrediting functions. (§99.31(a)(7))
- To parents of an eligible student if the student is a dependent for IRS tax purposes. (§99.31(a)(8))
- To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9))
- To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10)
- Information the school has designated as "directory information" under §99.37. (§99.31(a)(11))

SAMPLE DISTRICT POLICY – DATA PRIVACY 2

Family Educational Rights and Privacy Act (FERPA)
Model Notice for Directory Information

The Family Educational Rights and Privacy Act (FERPA), a federal law, requires that **[District]**, with certain exceptions, obtain your written consent prior to the disclosure of personally identifiable information from your child's education records. However, **[District]** may disclose appropriately designated "directory information" without written consent, unless you have advised the district to the contrary in accordance with district procedures. The primary purpose of directory information is to allow the **[District]** to include this type of information from your child's education records in certain school publications. Examples include:

- **A playbill, showing your student's role in a drama production;**
- **The annual yearbook;**
- **Honor roll or other recognition lists;**
- **Graduation programs; and**
- **Sports activity sheets, such as for wrestling, showing weight and height of team members.**

Directory information, which is information that is generally not considered harmful or an invasion of privacy if released, can also be disclosed to outside organizations without a parent's prior written consent. Outside organizations include, but are not limited to, companies that manufacture class rings or publish yearbooks. In addition, two federal laws require local educational agencies (LEAs) receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA) to provide military recruiters, upon request, with the following information – names, addresses, and telephone listings – unless parents have advised the LEA that they do not want their student's information disclosed without their prior written consent.[3]

If you do not want **[District]** to disclose directory information from your child's education records without your prior written consent, you must notify the district in writing by [insert date]. **[District]** has designated the following information as directory information: [Note: an LEA may, but does not have to, include all the information listed below.]

- **Student's name**
- **Address**
- **Telephone listing**
- **Electronic mail address**
- **Photograph**
- **Date and place of birth**
- **Major field of study**
- **Dates of attendance**
- **Grade level**
- **Participation in officially recognized activities and sports**
- **Weight and height of members of athletic teams**
- **Degrees, honors, and awards received**
- **The most recent educational agency or institution attended**
- **Student ID number, user ID, or other unique personal identifier used to communicate in electronic systems that cannot be used to access education records without a PIN, password, etc.[4]**

[3] These laws are: Section 9528 of the Elementary and Secondary Education Act (20 U.S.C. § 7908) and 10 U.S.C. § 503(c).

[4] A student's SSN, in whole or in part, cannot be used for this purpose.

SAMPLE DISTRICT POLICY – DATA PRIVACY 3

Issued October 9, 2002

Access to High School Students and Information on Students by Military Recruiters

Q. ***What are the recent changes made by Congress concerning military recruitment of high school students?***

A. Congress has passed two major pieces of legislation that generally require local educational agencies (LEAs) receiving assistance under the Elementary and Secondary Education Act of 1965 (ESEA) to give military recruiters the same access to secondary school students as they provide to postsecondary institutions or to prospective employers. LEAs are also generally required to provide students' names, addresses, and telephone listings to military recruiters, when requested.

Q. ***Where are these statutory requirements found?***

A. These requirements are contained in § 9528 of the ESEA (20 U.S.C. § 7908), as amended by the No Child Left Behind Act of 2001 (P.L. No. 107-110), the education bill Congress recently passed. These requirements are also contained in 10 U.S.C. § 503, as amended by § 544 of the National Defense Authorization Act for Fiscal Year 2002 (P.L. No. 107-107), the legislation that provides funding for the nation's armed forces in fiscal year 2002.

Q. ***What is the effective date for these military recruiter access requirements?***

A. While there are differences in the effective date provisions for 10 U.S.C. § 503 and § 9528 of the ESEA, both provisions apply to all LEAs receiving ESEA funds by not later than July 1, 2002.

Q. ***What are the requirements of § 9528 of the ESEA?***

A. Each LEA that receives funds under the ESEA must comply with a request by a military recruiter or an institution of higher education for secondary students' names, addresses, and telephone numbers, unless a parent has "opted out" of providing such information. Section 9528 also requires LEAs that receive funds under the ESEA to provide military recruiters the same access to secondary school students as they generally provide to postsecondary institutions or prospective employers. For example, if the school has a policy of allowing postsecondary institutions or prospective employers to come on school property to provide information to students about educational or professional opportunities, it must afford the same access to military recruiters.

Q. ***Under § 9528 of the ESEA, what notification must LEAs provide to parents before disclosing names, addresses, and telephone numbers of secondary students to military recruiters and officials of institutions of higher education?***

A. Under FERPA, an LEA must provide notice to parents of the types of student information that it releases publicly. This type of student information, commonly referred to as "directory information," includes such items as names, addresses, and telephone numbers and is information generally not considered harmful or an invasion of privacy if disclosed. The notice must include an explanation of a parent's right to request that the information not be disclosed without prior written consent. Additionally, § 9528 requires that parents be notified that the school routinely discloses names, addresses, and telephone numbers to military recruiters upon request, subject to a parent's request not to disclose such information without written consent. A single notice provided through a mailing, student handbook, or other method that is reasonably calculated to inform parents of the above information is sufficient to satisfy the parental notification requirements of

both FERPA and § 9528. The notification must advise the parent of how to opt out of the public, nonconsensual disclosure of directory information and the method and timeline within which to do so.

Q. ***If an LEA has not provided notice relating to "directory information," may it release a student's name, address, and telephone number when requested by a military recruiter?***

A. As noted above, an LEA may provide a single notice regarding both directory information and information disclosed to military recruiters. If an LEA does not disclose "directory information" under FERPA, then it must still provide military recruiters access to secondary students' names, addresses, and telephone listings. In addition, the LEA must notify parents that they may opt out of this disclosure. In other words, an LEA that does not disclose "directory information" must nonetheless provide a notice that it discloses information to military recruiters. The notice must be reasonably calculated to inform parents.

Q. ***If a parent opts out of the public, non-consent disclosure of directory information (or any subset of such information), must the three data elements be released to military recruiters upon their request?***

A. If a parent opts out of providing directory information to third parties, the opt-out relating to name, address, or telephone number applies to requests from military recruiters as well. For example, if the opt-out states that telephone numbers will not be disclosed to the public, schools may not disclose telephone numbers to military recruiters.

Q. ***If the school does not list one or more of the three data elements (e.g., telephone number) among its directory information, may it release that information to military recruiters?***

A. If a school does not designate one or more of the three items as "directory information" under FERPA, it still must provide all three items to military recruiters upon request. Also, in that case, the school would have to send a separate notice to parents about the missing "directory information" item(s), noting an opportunity to opt out of disclosure of the information to military recruiters. An easier method, of course, would be for the school to designate all three items – name, address, and telephone listing – as "directory information."

Q. ***How are the requirements under § 9528 of the ESEA enforced?***

A. Schools that do not comply with § 9528 of the ESEA could jeopardize their receipt of ESEA funds.

Q. ***How does § 544 of the National Defense Authorization Act for Fiscal Year 2002 amend the former requirements under 10 U.S.C. § 503?***

A. Section 544 of the National Defense Authorization Act for Fiscal Year 2002 revises Title 10, Section 503(c) in several important ways. First, the recruiting provisions now apply only to LEAs (including private secondary schools) that receive funds under the ESEA. Second, these provisions now require access by military recruiters to students, under certain conditions, and to secondary school students' names, addresses, and telephone listings. Third, as discussed earlier, they require LEAs to notify parents of their right to opt out of the disclosure of their children's names, addresses, and telephone numbers and to comply with any such requests from the parents or the students.

Q. ***How are these requirements under 10 U.S.C. § 503 enforced?***

A. In addition to the potential for loss of funds under ESEA noted above for failure to comply with § 9528 of the ESEA, an LEA that denies a military recruiter access to the

requested information on students after July 1, 2002, will be subject to specific interventions under 10 U.S.C. § 503. In this regard, the law requires that a senior military officer (e.g., Colonel or Navy Captain) visit the LEA within 120 days. If the access problem is not resolved with the LEA, the Department of Defense must notify the state Governor within 60 days. Problems still unresolved after one year are reported to Congress if the Secretary of Defense determines that the LEA denies recruiting access to at least two of the armed forces (Army, Navy, Marine Corps, etc.). The expectation is that public officials will work with the LEA to resolve the problem.

Additionally, the Department of Defense has developed a national high school data base to document recruiter access. Presently, 95 percent of the nation's 22,000 secondary schools provide a degree of access to military recruiters that is consistent with current law.

Q. ***Are private schools subject to the military recruiter requirements?***
A. Private secondary schools that receive funds under the ESEA are subject to 10 U.S.C. § 503. However, private schools that maintain a religious objection to service in the Armed Forces that is verifiable through the corporate or other organizational documents or materials of that school are not required to comply with this law.

Q. **Where *can I get more information on the requirements of 10 U.S.C. § 503?***
A. The Office of the Secretary of Defense may be contacted for copies of the statute or questions relating to it. Please contact the Accession Policy Directorate as follows:

Director, Accession Policy
4000 Defense Pentagon
Washington, DC 20301-4000
Telephone: (703) 695-5529

Q. ***Where can I get more information on the requirements of § 9528 of the ESEA?***
A. The Family Policy Compliance Office (FPCO) in the Department of Education administers FERPA as well as § 9528 of the ESEA, as amended by the No Child Left Behind Act of 2001. School officials with questions on this guidance, or FERPA, may contact the FPCO at FERPA@ED.Gov or write to the FPCO as follows:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202-4605
Telephone: (202) 260-3887
Fax: (202) 260-9001
www.ed.gov/offices/OM/fpco

SAMPLE DISTRICT POLICY – DATA PRIVACY 4

Student Data Privacy Bill of Rights

In line with the President's Consumer Privacy Bill of Rights, **[District]** shall adhere to the following practices when collecting student data. These rights shall transfer from parents or legal guardians to students once the student is eighteen or attending college:

1. **Access and Amendment:** Students have the right to access and amend their erroneous, misleading, or otherwise inappropriate records, regardless of who collects or maintains the information.

   *There are gaps in current laws and proposed frameworks concerning students' access and amendment to their data. **[District}** or other entities that collect any student information shall provide student access to this information. This includes access to any automated decision-making rule-based systems (i.e., personalized learning algorithms) and behavioral information.*

2. **Focused collection**: Students have the right to reasonably limit student data that [**District]** collects and retains.

   ***[District]** should collect only as much student data as it needs to complete specified purposes. "Educational purposes" and "educational quality" are frequent examples of broad and fluid purposes that grant carte blanche to collect troves of student data. **[District]** shall endeavor to maintain a more focused data collection, for example, by specifying that the collection is necessary to "improve fifth grade reading skills" or "enhance college-level physics courses." In focusing student data collection for specific purposes, **[District]** shall consider the sensitivity of the data and the associated privacy risks.*

3. **Respect for Context:** Students have the right to expect that **[District]** will collect, use, and disclose student information solely in ways that are compatible with the context in which students provide data.

   ***[District]** shall never repurpose or allow repurposing of student data without express written student consent. This includes using student data to serve generalized or targeted advertisements. Note that the Education Department's guidance states that federal student privacy laws do not prohibit **[District]** "from allowing a provider acting as a school official from serving ads to all students in email or other online services." This allows service providers to repurpose the information. Schools provide private companies access to student data to help enhance education quality. When companies use this access for general marketing purposes, they have repurposed the student data and turned the classroom into a marketplace.*

4. **Security:** Students have the right to secure and responsible data practices.

   *Amid recent, large-scale student data breaches, **[District]** will increase its data safeguards to ward against "unauthorized access, use, destruction, or modification; and improper disclosure" as described in the CPBR. **[District]** will immediately notify schools, students, and appropriate law enforcement of any breach. **[District]** shall refrain from collecting information if it cannot adequately protect it. Securing student information also entails deleting and de-identifying information after it has been used for its initial and primary purposes (no secondary uses allowed!).*

5. **Transparency:** Students have the right to clear and accessible information privacy and security practices.

   ***[District]** shall publish the types of information it collects, the purposes for which the information will be used, and the security practices in place. **[District]** shall also publish algorithms behind its decision-making.*

6. **Accountability:** Students should have the right to hold schools and private companies handling student data accountable for adhering to the Student Privacy Bill of Rights.

   ***[District]** is accountable to enforcement authorities and students for violating these practices.*

California Business and Professions Code Section 22584

Chapter 22.2. Student Online Personal Information Protection Act

SECTION 1.

(a) An operator of an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes and was designed and marketed for K-12 school purposes shall comply with all of the following requirements:

(1) It shall not use, share, disclose, or compile personal information about a K-12 student for any purpose other than the K-12 school purpose and for maintaining the integrity of the site, service, or application.

(2) It shall not use, share, disclose, or compile a student's personal information for any commercial purpose, including, but not limited to, advertising or profiling.

(3) It shall not allow, facilitate, or aid in the marketing or advertising of a product or service to a K-12 student on the site, service, or application.

(4) It shall take all reasonable steps to protect the data at rest and in motion in a manner that meets or exceeds commercial best practices. An operator shall be deemed to be in compliance with this paragraph if the operator ensures the following:

(A) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

(B) Valid encryption processes for data in motion are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others that are Federal Information Processing Standards (FIPS) 140-2 validated.

(b) (1) An operator of an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes and the site, service, or application was designed and marketed for K-12 school purposes shall provide a notice to the operator of a secondary site, service, or application that is accessible through the noticing operator's site, service, or application that the secondary site, service, or application is used for K-12 school purposes on a site, service, or application designed and marketed for K-12 school purposes.

(2) An operator of a site, service, or application designed and marketed for K-12 school purposes shall comply with this section upon either receiving notice under paragraph (1) that the site, service, or application is used for K-12 school purposes or if the operator otherwise has actual knowledge that the site, service, or application is used for K-12 school purposes.

(3) An operator that fails to provide the notice required by paragraph (1) to a secondary site, service, or application shall be liable for the secondary site, service, or application's compliance with this section, unless that secondary site, service, or application had actual knowledge it was being used for K-12 purposes and was designed and marketed for K-12 school purposes.

(c) An operator of an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K-12 school purposes and that it was designed and marketed for K-12 school purposes shall delete a student's personal information if any of the following occurs:

(1) The site, service or application is no longer used for the original K-12 school purpose.

(2) The student requests deletion, unless it is being used at the direction of a school or district for legitimate educational purposes and is under the control of the school or district.

(3) The student ceases to be a student at the institution and the operator becomes aware the student is no longer a student, unless it is being used at the direction of a school or district for legitimate educational purposes and is under the control of the school or district.

(d) Notwithstanding subdivision (a), an operator of an Internet Web site, online service, online application, or mobile application may disclose personal information of a student if other provisions of federal or state law require the operator to disclose the information, and the operator complies with the requirements of federal and state law in disclosing that information.

(e) An "online service" includes cloud computing services.

(f) Notwithstanding subdivision (a), an operator of an Internet Web site, online service, online application, or mobile application may disclose personal information of a student for legitimate research purposes as required by state and federal law and subject to the restrictions under state and federal law.

(g) For purposes of this section, "personal information" shall mean any information or materials in any media or format created or provided by a student, or the student's parent or legal guardian, in the course of the student's, or parent's or legal guardian's, use of the site, service, or application or an employee or agent of the educational institution, or gathered by the site, service, or application, that is related to a student and shall include, but not be limited to, information in the student's educational record, the student's email address, first and last name, home address, telephone number, other information that permits physical or online contact of a specific individual, discipline records, test results, special education data, juvenile delinquency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, email messages, documents, unique identifiers, profile, search activity, location information, Internet Protocol (IP) address, metadata, any aggregation or derivative thereof, or any information gained through tracking, including login and logoff information, searches, typing, photos, voice recordings, and geolocation information.

(h) This section shall not be construed to limit the authority of a law enforcement agency to obtain any content or information from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction.

(i) It is not the intent of the Legislature for this chapter to apply to general audience Internet Web sites.

SECTION 2.

The provisions of this act are severable. If any provision of this act or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given 6effect without the invalid provision or application.

California Education Code 49073.6

SECTION 1. Section 49073.6 is added to the Education Code, to read:
49073.6
(a) For purposes of this section, the following terms have the following meanings:
(1) “Educational purposes” means for purposes that aid in instruction in the classroom or at home, or in classroom administration.
(2) (A) “Social media” means an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations.
(B) “Social media” shall not include 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.
(b) Notwithstanding any other law or regulation, a school district, county office of education, or charter school that considers a program to gather or maintain in its records any information obtained from social media of any enrolled pupil shall notify pupils and their parents or guardians about the proposed program and provide an opportunity for public comment at a regularly scheduled public meeting of the governing board of the school district or county office of education, or governing body of the charter school, as applicable, before the adoption of the program. The notification required by this subdivision may be provided as part of the notification required pursuant to Section 48980.
(c) Notwithstanding Section 49062, a school district, county office of education, or charter school that adopts a program pursuant to subdivision (b) shall do all of the following:
(1) Gather or maintain only information that pertains directly to school safety or to pupil safety.
(2) Provide a pupil with access to any information about the pupil gathered or maintained by the school district, county office of education, or charter school that was obtained from social media, and an opportunity to correct or delete such information.
(3) (A) Destroy information gathered from social media and maintained in its records within one year after a pupil turns 18 years of age or within one year after the pupil is no longer enrolled in the school district, county office of education, or charter school, whichever occurs first.
(B) Notify each parent or guardian of a pupil subject to the program that the pupil’s information is being gathered from social media and that any information subject to this section maintained in the school district’s, county office of education’s, or charter school’s records with regard to the pupil shall be destroyed in accordance with subparagraph (A). The notification required by this subparagraph may be provided as part of the notification required pursuant to Section 48980. The notification shall include, but is not limited to, all of the following:
(i) An explanation of the process by which a pupil or a pupil’s parent or guardian may access the pupil’s records for examination of the information gathered or maintained pursuant to this section.
(ii) An explanation of the process by which a pupil or a pupil’s parent or guardian may request the removal of information or make corrections to information gathered or maintained pursuant to this section.
(C) If the school district, county office of education, or charter school contracts with a third party to gather information from social media on an enrolled pupil, require the contract to do all of the following:
(i) Prohibit the third party from using the information for purposes other than to satisfy the terms of the contract.
(ii) Prohibit the third party from selling or sharing the information with any person or entity other than the school district, county office of education, charter school, or the pupil or his or her parent or guardian.
(iii) Require the third party to destroy the information immediately upon satisfying the terms of the contract.
(iv) Require the third party, upon notice and a reasonable opportunity to act, to destroy information pertaining to a pupil when the pupil turns 18 years of age or is no longer enrolled in the school district, county office of education, or charter school, whichever occurs first. The school district, county office of education, or charter school shall provide notice to the third party when a pupil turns 18 years of age or is no longer enrolled in the school district, county office of education, or charter school. Notice provided pursuant to this clause shall not be used for any other purpose.

California Education Code 49073.1

SECTION 1. Section 49073.1 is added to the Education Code, to read:

(a) A local educational agency may, pursuant to a policy adopted by its governing board or, in the case of a charter school, its governing body, enter into a contract with a third party for either or both of the following purposes:

(1) To provide services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

(2) To provide digital educational software that authorizes a third-party provider of digital educational software to access, store, and use pupil records in accordance with the contractual provisions listed in subdivision (b).

(b) A local educational agency that enters into a contract with a third party for purposes of subdivision (a) shall ensure the contract contains all of the following:

(1) A statement that pupil records continue to be the property of and under the control of the local educational agency.

(2) Notwithstanding paragraph (1), 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. Compliance with this requirement shall not, in itself, absolve the third party of liability in the event of an unauthorized disclosure of pupil records.

(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) 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.

(B) The requirements provided in subparagraph (A) shall 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 pursuant to paragraph (2).

(8) A description of how the local educational agency and the third party will jointly ensure compliance with the federal Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g).

(9) A prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising.

(c) In addition to any other penalties, a contract that fails to comply with the requirements of this section shall be rendered void if, upon notice and a reasonable opportunity to cure, the noncompliant party fails to come into compliance and cure any defect. Written notice of noncompliance may be provided by any party to the contract. All parties subject to a contract voided under this subdivision shall return all pupil records in their possession to the local educational agency.

(d) For purposes of this section, the following terms have the following meanings:

(1) "Deidentified information" means information that cannot be used to identify an individual pupil.

(2) "Eligible pupil" means a pupil who has reached 18 years of age.

(3) "Local educational agency" includes school districts, county offices of education, and charter schools.

(4) "Pupil-generated content" means materials created by a pupil, including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, and account information that enables ongoing ownership of pupil content. "Pupil-generated content" does not include pupil responses to a standardized assessment where pupil possession and control would jeopardize the validity and reliability of that assessment.

(5) (A) "Pupil records" means both of the following:

(i) Any information directly related to a pupil that is maintained by the local educational agency.

(ii) Any information acquired directly from the pupil through the use of instructional software or applications assigned to the pupil by a teacher or other local educational agency employee.

(B) "Pupil records" does not mean any of the following:

(i) Deidentified information, including aggregated deidentified information, used by the third party to improve educational products for adaptive learning purposes and for customizing pupil learning.

(ii) Deidentified information, including aggregated deidentified information, used to demonstrate the effectiveness of the operator's products in the marketing of those products.

(iii) Deidentified information, including aggregated deidentified information, used for the development and improvement of educational sites, services, or applications.

(6) "Third party" refers to a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records.

(e) If the provisions of this section are in conflict with the terms of a contract in effect before January 1, 2015, the provisions of this section shall not apply to the local educational agency or the third party subject to that agreement until the expiration, amendment, or renewal of the agreement.

(f) Nothing in this section shall be construed to impose liability on a third party for content provided by any other third party.