iKEEPSAFE
PEACE OF MIND FOR FAMILIES ONLINE

TOP 10 PRIVACY HACKS FOR EDUCATORS

This document walks educators through likely scenarios where student privacy needs to be considered. It is designed to increase student privacy awareness and improve privacy practices.

TABLE OF CONTENTS

4.14 Use an app or service that also tracks location
4.15 Report abuse or complaints to school officials
4.16 Digital library searches/Internet searches
4.17 Library books and videos that are checked
4.18 Cloud services that store student information

5. BYOD - My school allows students to bring devices to be used for educational purposes.

6. If I give students a device to take home?

7. I have student data on a device or service, so what do I need to know about deletion or disposal? Data retention and/or disposal?

8. When do educators need to notify parents or students?

9. When do educators need parent permission/consent?

10. Student data retention and/or disposal requirements

KEY:
BLUE = CALIFORNIA PRIVACY LAW
RED = FEDERAL PRIVACY LAW

1. I AM AN EDUCATOR THAT WANTS TO GATHER OR MONITOR INFORMATION ABOUT STUDENTS OR THEIR FAMILIES.

1.1. Is it sensitive information? If so, PPRA requires written permission.

PPRA 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, antisocial, 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.[1] SEAs/LEAs, and anyone using funds from the Dept of Ed is responsible (Dept of Ed enforces).

1.2. Is the information on social media? You will need to ask:

- What is the purpose of the monitoring?
- What information are you looking for and does it relate to the safety of the school and/or student?
- Have you given the appropriate notifications?
- Do you have the appropriate permissions?
- How will this information be used and stored?

Collection of Student Information from Social Media (California Education Code §49073.6 Pupil Records) applies. It requires notifying both students and parents, and allow for public comment. The search must be limited to information about the school and students' safety.

Disposal: Records from social media must be destroyed within a year of the student turning 18 or leaving the school system. SEAs/LEAs are responsible. The California Attorney General enforces this rule. (Blue text represents California privacy law).

2. I am a California educator and want to approve, renew, amend or accept a contract or term of service for technology that can access and/or collect student data.

Privacy of Pupil Records: 3rd-Party Digital Storage & Education Software, Education Code section 49073. (AB 1584) requires specific statements and descriptions be included in the contract. If all of the information is not included then the contract is rendered void. (Both LEAs and Vendors are responsible. The California Attorney General may enforce such contracts.)

California AB 1584 Compliance Checklist for School District/LEA Technology Services Agreements Technology services agreements entered into, amended, or renewed by a local education agency on or after January 1, 2015 must include 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.[2]

All of the following requirements must be **explicitly included in such contracts:**

DESCRIBE

1. Describe how students can control content created for education-related purposes, along with a way to transfer content to a personal account later.
2. Describe how parents, legal guardians, or students can review and correct personally identifiable information contained in their records.
3. Describe procedures for notifying affected parents, legal guardians, or eligible students in the event of unauthorized disclosure of student records.
4. Describe how LEAs and third parties will comply with FERPA
5. Outline actions that third parties will take to ensure student data is secure and confidential

STATE

1. Establish that the LEA owns and controls student records.
2. 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.

PROHIBIT

1. Prohibit third parties from using personally identifiable information from student records to target advertising to students.
2. Prohibit third parties from using student information for purposes outside of those named in the contract.

Here is a legal checklist:

- 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[3]

3. I AM AN EDUCATOR THAT WANTS STUDENTS UNDER 13 TO USE A COMMERCIAL TECH PRODUCT.

3.1. What will I need to do?

1. Gather all of the required COPPA notices from operator
2. Determine how you will ensure the PII is only used for educational purposes
3. Determine the mechanism to allow parents to review the personal information collected
4. Find out, from the vendor, how they will delete student PII after it is no longer needed for educational purposes
5. Provide direct notification to parents at least annually regarding the rights of the parents to opt their child out of activities that collect, disclose or use personal information from students to sell it or for marketing (or to allow others to do it)

Parents permission is required for educators to share PII with commercial operators and apps. The PII must be restricted to educational use. 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 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.

3.2. 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

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).

4. I WANT TO SHARE STUDENT PII INCLUDING SCHOOL RECORDS WITH ORGANIZATIONS AND INDIVIDUALS, OR I WANT TO SHARE INFORMATION WITH COMMUNITY GROUPS THAT PROVIDE TUTOR SERVICES OR HOMEWORK HELP.

4.1 Questions I should ask myself:

- What "type" of information do I want to share?
- Who will have access?
- Will I be the only one that has access?
- Will other teachers or educators have access?
- Will other students have access?
- Do I have the right permissions to share?
- How will it be shared?
- Will it be distributed electronically?
- Is any information from a student under 13?
- Have I documented the right information?
- Do I have a policy that allows it?

4.2. If registration is not required:

If I want to use a site or app that doesn't require signing in, I need to ask:

- What are the privacy policies?
- Do the privacy policies align with school policies?
- Will students be using this app?
- Do the privacy policies align with school policies?
- What information can be collected actively or passively?
- What is the age requirement?

4.3. If registration is required:

If I want to use software or site requires a sign on with a username and password, I need to ask:

- What are the privacy policies?
- Do the privacy policies align with school policies?
- What information is collected in registration?
- Does the information collected seem excessive for use?
- What is the minimum age requirement for use?
- Who will be registering for the account to obtain the screen name and password?
- Will students be creating individual accounts?
- Can the product be used for personal as well as educational purposes ?
- Are you registering students under the age of 13? If so, who is consenting on behalf of the child (school and/or parent)?
- What is the minimum age requirement for use?

4.4. App

If I want my student to use an app, then I need to consider:

- What student information can I share on an education app?
- What "type" of information do I want to share?
- What is the purpose of sharing?
- How will the information be used?
- Do I have the right permissions to share?

4.5. Online Game or app (personalized learning opportunity)

If I want my students to play an online game, use a homework app, or digital flashcards and I want to know how the students and the class are doing, then I should consider:

- Who within the classroom and/or home provides oversight?
- Is there an interactive element?
- Is the service "gated" so that students can only interact with others in the class?
- How is the interaction monitored by the service?
- If necessary, how is student information ported into the service?
- Are students using their actual names or a screenname?
- Does your school have an Acceptable Use Policy? Does it apply to using these types of services, even when students use it from home ?
- Do you have needed permissions?
- Are students aware of privacy implications and the importance of not over sharing pii in interactive environments?
- Does it require registration? If so, see registration above.

4.6. Chat/ Instant Message

I want my students (over and under the age of 13) to be able to chat (IM) with me and with other students. What do I need to consider?

- How is the chat monitored by the service?
- Who within the classroom and/or home provides oversight?
- Is the chat "gated" so that students can only chat with others in the class?
- Are chats open to anyone?

- Are chat logs stored?
- Are students using their actual names or a screenname?
- Does your school have an Acceptable Use Policy? Does it apply to using chat services, even when students use it from home ?
- Do you have needed permissions?
- Are students aware of privacy implications and the importance of not over sharing pii in these environments?
- Is the student under 13? if so, who is providing verifiable consent?
- Does it require registration? If so, see registration above.

4.7. Parent Communication

I want to share information with parents (e.g. grades, attendance, money in lunch account, discipline or behavior feedback). I should ask:

- How do parents register?
- How do you communicate to parents that the service is available for use?
- Can the student have access to the information as well?
- How is information ported over to the service?
- Do you have needed permissions? Do they align with school policies?
- What are the privacy policies?

4.8. Single sign on service

I want to use a single sign on service so my students don't have to manage so many usernames and passwords.

- Do I have the right permissions?
- How will information be ported over?
- Who will have oversight?
- Have you reviewed the privacy policies? Do they align with school policies?
- How will student information be protected?

4.9. Interact with an online tutor, both real-time and data communication

I want to interact with an online tutor, using both real-time and data communication. I should ask:

- How is the communication monitored by the service?
- Who within the classroom and/or home provides oversight?
- Are tutoring sessions logged? Who has access to the logs?
- What information can be shared between student and tutor?
- Are students using their actual names?
- Does your school have an Acceptable Use Policy? Does it apply to using the online tutoring, even when students use it from home?
- Do you have needed permissions?
- Are students aware of privacy implications and the importance of not over sharing pii in these environments?
- Does it require registration? If so, see registration above.

4.10. Use digital tools to manage create and share projects and school activities

Class Projects and Activities (e.g., Build Creative projects, graphic art projects, video, sound, with digital software; Share creative projects art, music, video, inventions, science projects, book reports; Manage class or school elections, Teacher and students communicating on a commercial service such as Google Docs)

- How do you track who is contributing what content?
- Is there oversight?
- Is the 'virtual environment' limited to users with the password (students/parents/admin)?
- Is the project/activity visible to anyone?
- If visible to anyone, are you using actual student names or initials/pseudonyms ?
- Do students have an identifiable profile? If so, who can view the profile?
- Can students interact in the virtual space? If so, see chat and IM above.
- Does your school have an Acceptable Use Policy? Does it apply to using virtual environments for class projects, even when students use from home?
- Do you have the necessary permissions?
- Where is the environment hosted?
- Does it require registration? If so, see registration above.

4.11. Use a social networking service like Twitter for school purposes (i.e. homework reminders, class discussions,or teachers/student communication)

- Is it being used for educational purposes?
- What are the privacy policies? Do they align with school policies?
- Is there oversight?
- Will it be used by students on an individual basis? Do they meet the posted age requirement?
- Does your school have an Acceptable Use Policy?
- Does it apply to using the social networks, even when students use it from home ?
- Do you have needed permissions?
- Are students aware of privacy implications and the importance of not over sharing PII in these environments?
- Does it require registration? If so, see registration above.

4.12. Use class blogs and individual student blogs for education purposes and extracurricular activities like school clubs and sports

- Is posting and commenting monitored and approved by the teacher ?
- Can the teacher/admin track who edits?
- Is the blog limited to users with the password (students/parents/admin)?
- Is the blog visible to anyone but comments are limited to user with the password ?
- If visible to anyone, are you using actual student names or initials/pseudonyms ?
- Do students have an identifiable profile? If so, who can view the profile?
- Can students upload images and videos to the blog ?
- Does your school have an Acceptable Use Policy? Does it apply to using blogs, even when students use from home ?
- Do you have the necessary permissions?

- Where is the blog hosted?
- Does it require registration? If so, see registration above.

4.13. Code, Open Source

Sign my student or class up for a global group online activity.

- Does it require a download?
- What are the privacy policies? Do they align with school policies?
- What information is collected actively or passively? (see registration section above)
- Is it a trusted source?
- How is the activity monitored?
- Are students using school-issued and/or home devices?
- Is it a collaborative coding activity? How do they students interact? Who do they interact with? Are the interactions monitored? Are the interactions stored?
- Are students aware of privacy implications and the importance of not over sharing pii in these environments?
- Does your school have an Acceptable Use Policy? Does it apply coding, even when students use from home?

4.14. Use an app or service that also tracks location

- Is it necessary? How does it relate to the service being provided?
- Can it be turned off?
- Who has provided verifiable consent? Per COPPA, geolocation that is “sufficient” to identify street name and name of city or town is considered PII (it doesn’t require actual address identification at the time of collection - e.g., longitude and latitude coordinates that are translated to a precise location on a map).

4.15. Report abuse or complaints to school officials

Some are internal (within the school), while others are external (e.g. police, fire, etc.)

- How is the information collected?
- How is this information protected?
- Are you sending potentially illegal images/videos that should not be sent?
- Are you confiscating personal devices (tablets, cell phones, etc)?
- Who has access to the reports, associated materials and/or devices?
- Where is the information being stored?
- Are you using a 3rd party to store or report abuse?
- What are the privacy policies of the 3rd party?
- Do you have policies and protocols in place?

4.16. Digital library searches/Internet searches

- Is there a block or filter in place to prevent access to obscene content, cp and other content harmful to minors? (CIPA)
- Are searches being tracked?
- If so, how is the data being used?

- Is it stored electronically using a 3rd party site or service?
- What are the privacy policies of the 3rd party?
- Do you have the required permissions to track?
- Are students and parents aware of the tracking?
- Does your school have an Internet safety policy in place that includes technological measures to prevent unwanted access to inappropriate material?

4.17. Library books and videos that are checked

- Are items (books, video and other content) that are checked out being tracked?
- If so, how is it that information being used?
- Is it stored electronically using a 3rd party site or service?
- What are the privacy policies of the 3rd party?
- Do you have the required permissions to track?
- Are students and parents aware of the tracking?

4.18. Cloud services that store student information

- Will I be the only one that has access?
- Will other teachers have access?
- Will other students have access?
- What type of information is stored?
- What information will I allow?
- What are the classroom rules about the service?
- What are the privacy policies of the cloud service?
- What are the contract terms of the cloud service?

5. BYOD - My school allows students to bring devices to be used for educational purposes.

- Does your school have a policy regarding BYOD?
- How do you address access to inappropriate content when students are using their own devices? (CIPA)
- How do you address troubleshooting personal devices within the school environment and potentially viewing personal (student and family), non-school related material on devices?
- What if you encounter inappropriate or even potentially illegal content on a personal device?
- Have you considered the UDID/persistent identifiers connected with an individual student using their own device? COPPA recognizes persistent identifiers, such as an UDID, that can be used to recognize a user over time and across different websites or online services as PII. This is important to remember when determining the need for verifiable consent to prior to collecting PII. Additionally, SOPIPA prohibits use of persistent identifiers to amass a profile about K-12 students except to further K-12 school purposes. Through the use of a BYOD there is more information connected directly to one child.

6. If I give students a device to take home?

- How will it be monitored? Filtering? AUP?
- Other family members that may access the device and store password or documents/images.

- What information belongs to the school? (Including information gathered from family members)
- How will you handle prohibited use by other family members?
- What policies must student and parents/guardian agree to? Does the policy address both prohibited activity as well as privacy implications?

7. I HAVE STUDENT DATA ON A DEVICE OR SERVICE, SO WHAT DO I NEED TO KNOW ABOUT DELETION OR DISPOSAL? DATA RETENTION AND/OR DISPOSAL? (CA PRIVACY LAW IN BLUE AND FEDERAL PRIVACY LAW IN RED)

- Social Networking law - destroy information within a year of students turning 18
- COPPA - delete data as soon as not needed for education purposes
- CA contract law - LEA can document and explain how the student data will not be retained or made available to third parties after the contract period has ended.
- SOPIPA - Delete a student's covered information if the school or district requests deletion of data under the control of the school or district.
- HIPAA - no mandate for how long records must be maintained
- FERPA - no mandate; FERPA requires student records to remain under the direct control and maintenance of schools

8. WHEN DO EDUCATORS NEED TO NOTIFY PARENTS OR STUDENTS?

- When monitoring social networks for student or school information. Social Networking law: Notify with public comment when gathering information from Social Networks (LEA)
- Data Breach Notification: (Both Vendor and LEA - CA Attorney General) Federal & State

9. WHEN DO EDUCATORS NEED PARENT PERMISSION? CONSENT FROM PARENTS IS REQUIRED WHEN:

- A student under 13 child participates on a commercial web platform or app that collects specific PII. COPPA requires verified parental consent before a commercial entity can collect PII. An educator can act in lieu of a parent but the data shared with the vendor must be limited to "educational purposes." The vendor is responsible to ensure consent but educator responsible to notify vendor and ensure student's data is used only for educational purposes. The FTC enforces.
- Gathering sensitive information from students or their families (survey, research) (PPRA)
- FERPA & HIPAA - sharing limited amounts of information (specified exceptions are established. FERPA supersedes HIPAA in many school situations)

10. STUDENT DATA RETENTION AND/OR DISPOSAL REQUIREMENTS

- Social Networking law - destroy information within a year of students turning 18
- COPPA - delete data as soon as not needed
- CA contract law requires that LEA can document and explain how the student data will not be retained or made available to third parties after the contract period has ended.
- SOPIPA Delete a student's covered information if the school or district requests deletion of data under the control of the school or district.
- HIPAA - no mandate for how long records must be maintained
- FERPA - no mandate; requires student records to remain under the direct control and maintenance of school

References

[1] Protection of Pupil Rights Amendment (PPRA) - Summary of Requirements. (n.d.). Retrieved from http://familypolicy.ed.gov/content/ppra-requirements.

[2] Data Privacy Guidebook: Privacy Guidelines and Practical Tips. (2015). f3law.com/privacy.

[3] Ibid.