Ready for School

Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data

November 2016

Kamala D. Harris, Attorney General
California Department of Justice

Ready for School

Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data

November 2016

Kamala D. Harris, Attorney General
California Department of Justice

Privacy Enforcement and Protection Unit
California Department of Justice
www.oag.ca.gov/privacy

Table of Contents

Message from the Attorney General

In the information age, technology holds the potential to unlock countless new opportunities to educate students for the workforce of tomorrow. And while we want to encourage technology in the classroom, we must be aware that student information is something that must be handled with great care. Organizations that make use of student data must take every step possible to be transparent with parents and schools and to protect student privacy. As the devices we use each day become increasingly connected, it's critical that we implement robust safeguards for what is collected, how it is used, and with whom it is shared. This guide is intended to offer recommendations to ensure privacy protections for students while making the most of technological advancements.

Sincerely,

Kamala D. Harris
Attorney General of California

Executive Summary

Technology has the potential to bring significant benefits to the education of our children. In recent years, we have seen widespread adoption of education technology (Ed Tech) in schools nationwide, with the U.S. market for PreK-12 estimated at $8.38 billion in 2015, according to the Software & Information Industry Association.

Ed Tech includes administrative management systems and tools, such as cloud services that store student data; instructional support, such as testing and assessment; and content, including curriculum and resources such as websites and mobile apps. Adaptive learning methods, enabled by technology and fueled by data, hold great promise for improving student learning.

While the vision of student-centered education empowered by innovative technology is compelling, as in other arenas, technology in schools brings certain risks and challenges along with new opportunities. The data on students collected and maintained by Ed Tech can be very sensitive, including medical histories, social and emotional assessments, child welfare or juvenile justice system involvement, progress reports, and test results. Furthermore, Ed Tech collects new types of data, such as metadata like a student's location and the type of device being used, which were not contemplated and may not be covered by longstanding federal laws on student and children's privacy.

Concerned about privacy risks and the gaps in existing laws, parents and policymakers in California responded by enacting two student privacy laws in 2014. One law applies to local educational agencies (such as school districts and charter schools) and requires specific terms to be included in contracts for services and software that store or collect student data. The other, the Student Online Personal Information Privacy Act (known as SOPIPA), imposes obligations on the companies that provide Ed Tech.

Protecting our children when they are online includes ensuring the privacy of their information as they learn. The Attorney General's Privacy Enforcement and Protection Unit has developed *Ready for School: Recommendations for the Ed Tech Industry to Protect the Privacy of Student Data* to promote the development of privacy best practices. The intent of the recommendations is to encourage Ed Tech to focus on educational purposes, by limiting the collection and use of the student information acquired through the technology.

In developing our recommendations, which focus broadly on student data, we consulted with a wide range of stakeholders including the Ed Tech industry, educators, and privacy and consumer advocates. We appreciate their perspectives and contributions.

Highlights of Recommendations

Data Collection and Retention: Minimization is the goal.

- Collect only the student information necessary to accomplish the school purposes your site or service is designed to achieve.
- Retain student information acquired through your site or service only as long as allowed or required by the school or district. Your default retention period for "covered information" should not be indefinite.
- If you link or direct student users of your site or service to external, non-Ed Tech sites or services, disclose any such referrals in your Privacy Policy. If you are also the operator of the external site or service, maintain the same privacy and security protections for student users when they leave your Ed Tech site or service.

Data Use: Keep it educational.

- Do not use any information acquired through your site or service as a basis for targeting advertising to a specific student or other user. This includes both advertising delivered on the site or service that acquired the information and advertising delivered on any other site or service.
- Do not use any information acquired through your site or service to create profiles of students, except profiles that are necessary for the school purposes furthered by your site or service.

Data Disclosure: Make protections stick.

- Contractually require your service providers who receive covered information acquired through your site or service to use the information only to provide the contracted service,

not to further disclose the information, to implement and maintain reasonable security procedures and practices as required by law, and to return or delete covered information at the completion of the contract.

- Do not sell any student information acquired through your site or service, except as part of a merger or acquisition. In such cases, ensure that any successor entity is contractually obligated to comply with the terms of your privacy policy under which the student information was collected, and with all legal requirements for the use, disclosure, and security of the student information previously acquired through your site or service.

Individual Control: Respect users' rights.

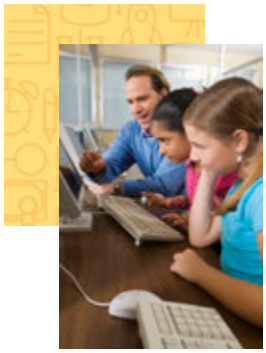
- Implement policies and procedures to allow parents, legal guardians, or eligible students (over 18 years old) to review their covered information acquired or maintained by your site or service.
- Implement policies and procedures to allow students to download, transfer, export, or delete their own student-created content.

Data Security: Implement reasonable and appropriate safeguards.

- Implement and maintain reasonable security measures appropriate to the nature of the student information acquired through your site or service. As we discussed in our recent *California Data Breach Report,* the Center for Internet Security's Critical Security Controls is a good starting point for high-priority security controls.
- Develop and describe your process for notifying schools or school districts, parents, legal guardians, or eligible students, as well as any appropriate government agencies, of any unauthorized disclosure of student information. Determine whether the incident and the types of data involved also require notification under California's breach notification law, and if so, take appropriate action.
- Implement a training program to ensure that employees understand your policies and procedures and also understands their individual obligations regarding the handling of student data and other personal information. Include data breach reporting procedures.

Transparency: Provide a meaningful privacy policy.

- The Policy should be complete and comprehensive, addressing at least all of the practices described in these recommendations.
- Be prepared to provide a copy of or link to the Policy to a school or district for posting on their website, to make it available to parents.
- Consider engaging with users (parents, educators, eligible students) to test and improve your Policy's comprehensibility.



Introduction

The Attorney General's Office has prepared this best practices guide in an effort to ensure that student privacy is respected, protected, and prioritized as the education technology industry brings learning innovations to our schools.

Education Technology: New Tools, New Challenges

The effective use of technology has the potential to bring significant benefits to the education of our children. Education technology (Ed Tech) can support administrators, teachers, and students. It can improve school operations and save money, support educators in their efforts to provide individualized learning, and allow teachers and parents to monitor students' progress inside and outside the classroom.

In recent years we have seen widespread adoption of Ed Tech in K-12 schools nationwide, spurred by initiatives at the national and state levels. The Software & Information Industry Association, the principal trade association for the Ed Tech industry, has reported steady growth in the industry for the past four years, with a 2015 estimate of the U.S. market for PreK-12 of $8.38 billion.[1] This figure does not include hardware or network infrastructure costs, both significant components of the Ed Tech industry.

"[T]he conversation has shifted from whether technology should be used in learning to how it can improve learning to ensure that all students have access to high-quality educational experiences."

National Education Technology Plan

National initiatives like the White House's ConnectED initiative[2] and the U.S. Department of Education Office of Educational Technology's 2016 National Education Technology Plan have all pushed for even greater adoption of Ed Tech. As the latter report remarks, "[t]he conversation has shifted from *whether* technology should be used in learning to *how* it can improve learning to ensure that all students have access to high-quality educational experiences."[3]

There are three basic types of Ed Tech: (1) administrative management systems and tools, such as cloud services that store student data, scheduling, and central office systems;

(2) instructional support, including testing and assessment, and professional development; and (3) content, including curriculum and resources such as websites and mobile apps.[4]

Key concepts central to understanding Ed Tech's potential contribution to improving educational outcomes are personalized learning and adaptive learning. Personalized learning, or learner-centered instruction, is a long-established tenet of good teaching, involving adapting to a student's unique goals, interests, and abilities.[5] It can be achieved in a variety of ways, with or without the use of technology. Examples of personalized learning include small group instruction and computer-based tutoring.

"While technology is a powerful tool for teaching and learning, it is imperative that students' personal information is protected at all times."

Otha Thornton, President, National PTA

Adaptive learning is a technology-enabled and data-driven approach to personalization, with the potential to improve student learning by deepening engagement, customizing assignments, and allowing instructors to make better use of class time.[6] Research on the effectiveness of Ed Tech is still limited, however, and the U.S. Department of Education calls for building the capacity to generate evidence of outcomes.[7] Companies that make exaggerated claims about their educational effectiveness can run afoul of consumer protection laws and face significant legal consequences.[8]

As in other arenas, along with opportunities, technology also brings certain risks and challenges, particularly related to the sensitive data that Ed Tech collects from the students, educators, and parents who use it. The president of the National PTA cautioned in 2014, "While technology is a powerful tool for teaching and learning, it is imperative that students' personal information is protected at all times."[9]

The administrative tools that maintain vast stores of student data have posed governance challenges for school districts. A 2013 study by the Fordham Law School found that 95 percent of school districts nationwide relied on cloud services to maintain and manage student data. The study also found that the services were weakly governed, with 20 percent of districts failing to have policies for their use of cloud services. Fewer than 25 percent of the agreements between districts and cloud providers specified the purpose for disclosures of student data and fewer than seven percent restricted the sale or marketing of the data.[10]

Schools and districts also face new challenges in managing the free online educational services, such as mobile apps, often used by teachers and staff. Increasingly districts have

a regular process for evaluating and acquiring educational services, including imposing contractual obligations on the provider. But free online services with clickwrap agreements can evade the process, forgoing not only a full evaluation of educational effectiveness, but also the consideration of privacy and security implications. The U.S. Department of Education, in a report available on its Privacy Technical Assistance Center (PTAC), recommends that schools have policies and procedures to evaluate and approve proposed online educational services and that free services be subject to the same process as paid educational services.[11]

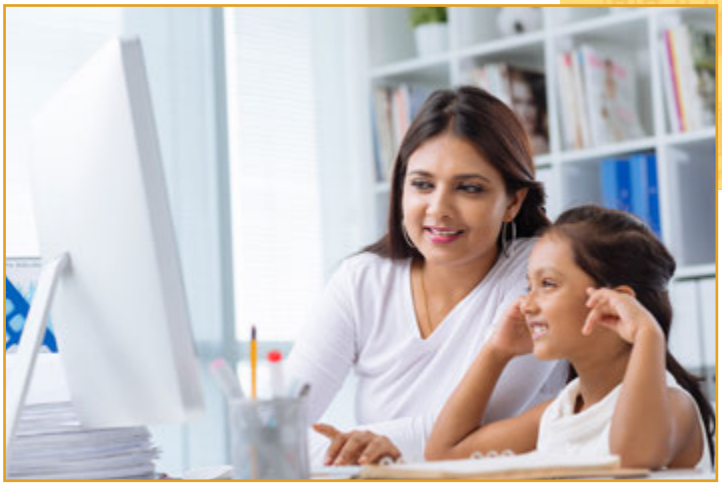
The data on students collected and maintained by Ed Tech can be extremely sensitive, including medical histories, social and emotional assessments, progress reports, and test results. Online services also collect new types of data, which were not contemplated by and may not be protected by federal privacy laws.[12] New data types collected by Ed Tech include "metadata," such as a student's location, how many attempts a student made to answer a question, and whether a student is using a desktop or a mobile device. Metadata can be put to good use to personalize learning and to improve educational products. It can also be used to influence or market to students or to their parents.

The line between personalized learning and marketing is one that must be clearly drawn in the use of Ed Tech. Organizations such as Common Sense Media have called for a School Privacy Zone, where students' personal information is used only for educational purposes and is appropriately secured.[13] The Future of Privacy Forum and the Software & Information Industry Association have introduced the Student Privacy Pledge, signed by over 300 companies that have agreed not to use student data collected through Ed Tech to target advertising to students and to secure student data.[14] It is only by protecting student privacy that we can ensure that our children will benefit from the transformative potential of Ed Tech, without opening themselves to the possibility of invasive marketing, identity theft, or disclosure of highly sensitive information.

Federal Student Privacy Laws

Two federal laws – the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Children's Online Privacy Protection Act of 1998 (COPPA) – govern the collection and use of student data. These privacy laws are widely viewed as having been significantly outdated by new technology.

FERPA



FERPA applies to educational agencies and institutions that receive federal funding from the U.S. Department of Education.[15] FERPA protects the confidentiality of education records, as defined, and provides parents and eligible students (at least 18 years old or attending a post-secondary school) with four basic rights. These are the following: (i) the right to review educational records, (ii) the right to correct or delete inaccurate information in records, (iii) the right to limit disclosure of records containing personally identifiable information, and (iv) the right to file a complaint about non-compliance with the Department of Education. FERPA is enforced by the Department of Education and violation is punishable by the withholding of federal funding from a violating school or program.

The Protection of Pupil Rights Amendment (PPRA) to FERPA provides parents with rights regarding surveys conducted by schools.[16] It requires schools that receive federal funds to obtain written consent from parents before administering surveys funded by the Department of Education that include sensitive information, such as political beliefs, psychological problems, sexual behavior or attitudes, or religious practices or beliefs. PPRA also provides rights regarding surveys funded by third parties, requiring schools, in consultation with parents, to adopt policies for parental access to and the use and protection of survey data. A 2001 amendment gives parents additional rights with regard to the surveying of minor students, the collection of information from students for marketing purposes, and certain non-emergency medical examinations.[17]

In recent years, the Department of Education has issued guidance for schools on protecting student privacy while using online educational services. Among other things, the guidance

says that if a school or district allows online educational service providers to collect student information under FERPA's school official exception, the provider cannot use the FERPA-protected information for any purpose, specifically citing marketing and targeting advertisements to students, other than the purpose for which the information was disclosed.[18]

Developments in Ed Tech appear to have outpaced many of FERPA's student privacy protections. The law's definition of educational records is not sufficiently broad to cover all student data now collected by Ed Tech, in particular metadata.[19] Furthermore, FERPA's many exceptions complicate and undermine some of its protections and the severity of its only enforcement mechanism has resulted in no instances of funds withheld from any institution or program as the result of violation.[20]

COPPA

Another federal law, the Children's Online Privacy Protection Act of 1998 (COPPA), also has implications for the privacy of younger students. COPPA applies to operators of websites and online services that are directed to children under the age of 13 and that collect personal information from the children.[21] It also applies to operators of general audience sites and services that have actual knowledge that they collect personal information from children under 13. COPPA requires such operators to do the following: (i) provide notice to parents, (ii) obtain verifiable consent from parents before collecting personal information from children, (iii) manage disclosures to third parties, (iv) limit retention of children's personal information, (v) enable parents to review and delete their children's personal information and prevent further use or collection of it, (vi) secure children's personal information, and (vii) post a privacy policy. COPPA is enforced by the Federal Trade Commission, with civil penalties of up to $40,000 per violation; state attorneys general are also authorized to bring a civil action for injunctive relief, damages or other compensation, or other appropriate relief.

In 2015, the FTC updated its COPPA compliance guidance, including addressing the circumstances under which educational institutions can provide consent, in loco parentis, for Ed Tech programs to collect personal information from students.[22] Noting that FERPA requirements and state laws protecting student data must also be complied with, the FTC says that an Ed Tech operator that is under contract with a school may rely on the school's consent to collect personal information from students for the use and benefit of the school and for no other commercial purpose.

Like FERPA, COPPA has limitations in protecting student data privacy. COPPA applies only to personal information collected directly *from* children, not information about them provided by other parties. It only covers children under the age of 13, and thus does not apply to many middle school and high school students.

California Student Privacy Laws

Concerned about privacy risks and the weaknesses in existing laws, parents and policymakers have responded. In 2014, California enacted two student privacy laws intended to fill gaps in student data privacy protections: one on education agency contracts for Ed Tech and one, the Student Online Personal Information Privacy Act (SOPIPA), on the privacy practices of Ed Tech providers. Another law modeled on SOPIPA was enacted in 2016: the Early Learning Personal Information Protection Act (ELPIPA), which takes effect on July 1, 2017 and imposes the same requirements as SOPIPA on providers of Ed Tech for preschool or prekindergarten.[23]

Education Agency Contracts

The first new law authorizes local education agencies (county offices of education, school districts, and charter schools) to enter into contracts with third parties for data storage services or digital educational software that store, manage, access, or use pupil records.[24] It requires such contracts to include specific provisions regarding the use, ownership, and control of the pupil records.

The law's requirements for contracts include the following:

- A statement that pupil records continue to be the property of and under the control of the education agency.
- 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 for those required or specifically permitted by the contract.

- A description of the procedures by which a parent, legal guardian, or eligible pupil (i.e., one who is 18 years of age or older) may review personally identifiable information in the pupil's records and correct erroneous information.
- A description of the actions the third party will take 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 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.
- A description of how the agency and the third party will jointly ensure compliance with FERPA.
- A prohibition against the third party using personally identifiable information in pupil records to engage in targeted advertising.

The law provides that non-compliant contracts shall be rendered void if, upon notice and a reasonable opportunity to cure, the non-compliant party fails to come into compliance and cure any defect. Written notice of non-compliance may be provided by any party or by an intended beneficiary of the contract. Parties subject to a voided contract are required to immediately return all pupil records in their possession to the education agency.

SOPIPA

The other new law is the Student Online Personal Information Protection Act (SOPIPA), a groundbreaking law that requires Ed Tech providers to comply with baseline privacy and security protections. SOPIPA has received nationwide attention.[25] Soon after its passage in January 2015, President Obama released a legislative proposal based on SOPIPA and since then, Congress and state legislatures have been very active on the issue

of student privacy. In Congress, half a dozen bills have been introduced that range from creating a commission to study the issue, to proposals similar to SOPIPA, and amendments to FERPA. As of May 2016, 26 other states had introduced SOPIPA-style bills with seven of them enacted.[26]

SOPIPA applies to the operators of websites and online services, including apps and mobile apps, that are used primarily, designed, and marketed for K-12 school purposes, as defined. SOPIPA's purpose is to limit the collection and use of data, particularly student data, to school purposes.

While the law's focus is on student data privacy, some of its provisions apply to information from or about other users of the technology, such as parents, guardians, and educators. Other provisions apply only to "covered information," which is defined in the law as personally identifiable information or materials that are either i) created or provided by a student or parent or guardian through use of a site or service, ii) created or provided to an operator by educator, or iii) gathered by an operator through a site or service and describes or otherwise identifies a student.

Unlike FERPA, SOPIPA applies to industry and not to schools, and it specifically addresses new types of data and new methods of data collection. Unlike COPPA, SOPIPA does not provide a parental-consent exception and it applies to information on all K-12 students, regardless of their age.

SOPIPA contains specific prohibitions and obligations, including the following.

Operators are prohibited from:

- Engaging in targeted advertising based on any information, including persistent unique identifiers, acquired through the use of the technology.
- Using any information, including persistent unique identifiers, gathered through the technology to create profiles of students, except for K-12 school purposes.
- Selling student information.
- Disclosing covered information, except under specified circumstances. Specified exceptions include disclosure in furtherance of K-12 school purposes, provided that the recipient is required to meet specified security and deletion standards and does not further disclose the information (except to allow or improve operability and functionality with the student's classroom or school). Disclosure is also permitted to ensure legal compliance or respond to judicial process; to protect the safety of users or

others or security of the site; or to a service provider, subject to specified contractual obligations.

Operators are required to:

- Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information, to protect it from unauthorized access, destruction, use, modification, or disclosure.
- Delete a student's covered information if the school or district requests deletion of data under its control.

Operators are permitted to:

- Use student data for adaptive learning or customized student learning purposes.
- Disclose covered information for legitimate research purposes, if required by state or federal law or if allowed by state or federal law and under the direction of the educational agency, provided that no covered information is used for advertising or for profiling other than for K-12 school purposes.
- Disclose covered information to a local educational agency as permitted by law.
- Use de-identified student information within the operator's site or service to improve education products; to demonstrate the effectiveness of the operator's products; and, in aggregated form, for the development and improvement of eductional sites and services.

This law does not apply to general audience sites or services, nor does it limit internet service providers from providing connectivity to schools, students, or their families.

Recommended Practices: Purpose and Scope

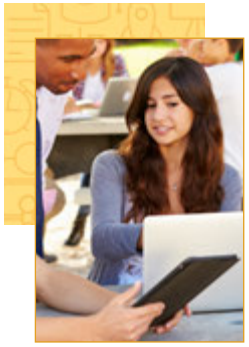
The Attorney General's Privacy Enforcement and Protection Unit has the mission of protecting the inalienable right to privacy conferred by the California Constitution. The Privacy Unit enforces state and federal privacy laws and develops programs to educate individuals, businesses and organizations on privacy obligations, rights, and best practices.

Protecting our children when they are online includes ensuring the privacy of their information as they learn. These recommendations are intended to encourage companies whose Ed Tech products enter the physical or virtual classroom to model the good digital citizenship that our students are being taught by protecting their personal information and using it only for school purposes.

The recommendations here are not regulations, mandates, or legal opinions. Rather, they are part of an effort to encourage the development of privacy best practices.

While there are differences in the specific provisions of privacy laws applicable to Ed Tech companies, we believe it is possible to chart a high road of best practices aimed at achieving the intended result of protecting student data privacy. It is only by doing so that we will be able to make appropriate use of technology in building a learning system for the current century.

In preparing this document, the Privacy Unit consulted numerous stakeholders, including educators, Ed Tech providers, parents, academics, and privacy advocates. We appreciate their insights and contributions.



Recommendations

The intent of these recommendations, like that of the new California student data privacy laws described in the Introduction, is to ensure that educational technology is focused on educational purposes, by limiting the collection and use of the student information collected through and maintained by Ed Tech. It should be noted that SOPIPA refers to several types of information in mandating how operators use and protect data. For example, the law refers to "any information" acquired through the use of Ed Tech, whether by a student, parent, guardian, teacher or other educator. In other provisions, the law refers to "student information" and in some more narrowly to "covered information," which is explicitly defined in the statute.[27] In general, our recommendations focus broadly on information collected from and about students and we specify when addressing covered information more narrowly.

These recommendations are directed to the Ed Tech industry, specifically to operators of websites and online services with actual knowledge that a site or service is used primarily for K-12 school purposes and that marketed it for such purposes. Online services include, but are not limited to, mobile applications and cloud computing services.

The recommendations here are also relevant for providers of Ed Tech for preschool or pre-kindergarten purposes.[28] The use of the terms "student" and "school" should be understood to include "pupil" and "preschool or kindergarten," respectively.

Data Collection and Retention: Minimization is the Goal

- *Describe the Data Collected:* Describe the types or categories of student information that you acquire from schools, school districts, teachers, parents, or students. Data types may include behavioral data reflecting how a student used the site or service or what content the student has accessed or created through it, and transactional data, such as persistent unique identifiers, collected through the use of your site or service. While unique identifiers are evolving with technology, currently such identifiers include, but are not limited to, cookies, device IDs, IP addresses, and other data elements if used to identify devices or users.

- *Data Collection Methods:* Describe how you collect the various data types, such as through a student's use of the technology, from content provided by a student, or from content provided by a district, school, teacher, or other educator.
- *Data Minimization:* Collect only the student information necessary to accomplish the school purposes your site or service is designed to achieve or as directed by the school or district.
- *Direction to Other Sites or Services:* If you link or direct student users of your site or service to external, non-Ed Tech sites or services, disclose any such referrals in your Privacy Policy and, where possible, include a link to the privacy policy of the referral site or service. If you are also the operator of the external site or service, maintain the same privacy and security protections for your student users when they leave your Ed Tech site or service.
- *Data Retention:* Retain student information acquired through your site or service only as long as allowed or required by the school or district.[29] Describe your data retention policy, including how long you retain student information and why. Your default retention period for covered information should not be indefinite.
- *Data Destruction:* Build into your system the ability to destroy personally identified or identifiable information acquired through your site or service. Be prepared to delete the information if so directed by the school or district.

Data Use: Keep it Educational

- *Describe* the purposes for which you use the different types of student information acquired through your site or service.
- *Targeted Advertising:* Do not use ***any*** information, including covered information and persistent unique identifiers, acquired through your site or service as a basis for targeting advertising to a specific student or other user. This includes both advertising delivered on the site or service that acquired the information and advertising delivered on any other site or service based on that information.

- *Profiling:* Do not use ***any*** information, including covered information and persistent unique identifiers, acquired through your site or service to create profiles of students, except profiles that are necessary for the school purposes furthered by your site or service.

- *Product Improvement:* If you use student information acquired through your site or service to develop or improve your educational products or to demonstrate their effectiveness, aggregate or de-identify the data first. See the guidance on data aggregation and de-identification from the U.S. Department of Education and the National Center for Education Statistics and a white paper on de-identification and student data from the Future of Privacy Forum.[30]

Data Disclosure: Make Protections Stick

- *Describe* the types of third parties to which you disclose covered information acquired through your site or service and the purposes for such disclosures. Be specific. For example, describe the types of entities (such as educational agencies, researchers, service providers, other companies) to which you disclose covered information for any of the purposes discussed below.

- *Disclosure for School Purposes:* Only disclose covered information acquired through your site or service when doing so furthers the specific school purposes of your site or service. Ensure that any such recipient does not further disclose the information except in furtherance of those purposes and is obligated to meet legal requirements to secure the information.[31]

- *Disclosure for Research Purposes:* Only disclose covered information for research purposes if required by state or federal law and subject to the restrictions of such laws, or if disclosure for research purposes is allowed by state or federal law and is under the direction of a school, district or state education department. In neither case should covered information be used for advertising or for profiling a student other than for school purposes.

- *Disclosure to Service Providers:* Contractually require your service providers who receive covered information acquired through your site or service to use the information only to provide the contracted service, not to further disclose the information, to implement and maintain reasonable security procedures and practices as required by law, and to return or delete covered information at the completion of the contract. Include a requirement that your service providers notify you immediately of any unauthorized disclosure of the student information in their custody, and then act promptly to provide proper notice as required by law.[32] Make clear to service providers that they may separately face liability for the mishandling of student data.

- *Disclosure for Product Improvement:* If you share covered information for the development and improvement of educational sites or services, de-identify and aggregate the information first.[33]
- *Disclosure for Other Purposes:* Other than the disclosures described above, only disclose covered information acquired through your site or service to ensure legal compliance, respond to judicial process, or protect individuals' safety or the security of the site or service.
- *Monitoring and Control:* Control the information disclosed through your site or service by monitoring for the presence of unauthorized third parties or third parties with unauthorized information collection practices. Take action to remove any unauthorized parties.
- *Sale:* Do not sell any student information acquired through your site or service, except as part of a merger or acquisition. In such cases, ensure that any successor entity is contractually obligated to comply with the terms of your privacy policy under which the student information was collected, and with all legal requirements for the use, disclosure, and security of the student information previously acquired through your site or service.

Individual Control: Respect Users' Rights

- *Describe* the procedures for a parent, legal guardian, or eligible student to review and correct covered information.
- *Access:* Implement policies and procedures to allow parents, legal guardians, or eligible students to review their covered information acquired or maintained by your site or service.
- *Correction:* Implement policies and procedures to allow parents, legal guardians, or eligible students to correct errors in their covered information acquired or maintained through your site or service.
- *Student-Created Content:* Implement policies and procedures to allow students to download, transfer, export, or delete their own student-created content. Use the Privacy Policy as one place to provide information on how a student can do this[34]

Data Security: Implement Reasonable and Appropriate Safeguards

- *Provide a general description* of the technical, administrative and physical safeguards you use to protect student information from unauthorized access, destruction, use, modification, or disclosure.

- *Reasonable and Appropriate Security:* Implement and maintain reasonable security measures appropriate to the nature of the student information, including covered information, acquired through your site or service. Designate and train someone responsible and use a risk management process: identify your data assets, assess threats and vulnerabilities, apply appropriate controls, monitor their effectiveness, and repeat the process. As we discussed in our recent *California Data Breach Report*, the Center for Internet Security's Critical Security Controls is a good starting point for high-priority security controls.[35] The Federal Trade Commission's Start with Security also offers helpful guidance.[36]
- *Data Breach Notification:* Develop and describe your process for notifying schools or school districts, parents, legal guardians, or eligible students, as well as any appropriate government agencies, of any unauthorized disclosure of student information. Determine whether the incident and the types of data involved also require notification under California's breach notification law, and if so, take appropriate action.[37]
- *Employee Privacy and Security Training:* Implement a training program to ensure that employees understand your policies and procedures and also understand their individual obligations regarding the handling of student data and other personal information. Include data breach reporting procedures.

Transparency: Provide a Meaningful Privacy Policy

- *Scope:* The Privacy Policy should cover all student information, as well as the personally identifiable information of other users (parents, guardians, educators), acquired through your site or service.[38] The Policy should be complete and comprehensive, addressing at least all of the practices described in these recommendations. Consider a layered-notice format to highlight major elements.[39]
- *Availability:* Make the Policy recognizable by giving it a descriptive title, such as "Privacy Policy" or "Data Collection and Use Policy." Make the Privacy Policy available in a single location; don't make users search for it in Terms of Service or Terms and Conditions statements, for example.

Make the Policy conspicuously available on your website or from within your mobile app or other online service.[40] If your app is available through an online store or other

platform, also provide a link to the Policy there so that potential users can review it before downloading the app.

Be prepared to provide a copy of or a link to the Policy to a school or school district for posting on their website. Schools and districts are increasingly receiving requests from parents to share the privacy policies of the online services they use.

- *Readability:* Make the Privacy Policy for your site or service easy for parents and educators to understand. Use plain language, for example, say what you currently do or don't do, instead of what practices you "may" employ at some future time. If there are practices that you only employ in some circumstances, specify those circumstances. Be concrete and specific about the data practices related to all the features of your site or service, explaining where appropriate that a school or district may choose not to use all of its features. Format the Policy with headers that identify key parts of the policy, such as Information We Collect, How We Use Your Information, Information We Share, Access to Your Information, Security, Effective Date, and Privacy Contact.
- *User Testing:* Consider engaging with users (parents, educators, eligible students) to test your Policy's comprehensibility and modify it to reflect their feedback.
- *Effective Date and Notice of Change:* Provide the effective date of your Privacy Policy. Describe how you will provide notice before making material changes to your Policy to the appropriate "account holder," that is, the school or district, parent, or eligible student.
- *Privacy Contact:* Provide a way for schools or districts, parents or legal guardians, and eligible students to contact you with questions or concerns about your privacy practices. Provide at a minimum an email address and consider providing a toll-free phone number as well. Develop and train staff in procedures for receiving and responding to privacy concerns.

Appendices

CALIFORNIA EDUCATION CODE SECTION 49073.1

49073.1. (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.

California Business and Professions Code Sections 22584-22585 Student Online Personal Information Protection Act (SOPIPA)

22584. (a) For the purposes of this section, "operator" means the operator of an Internet Web site, online service, online application, or mobile application with actual knowledge that the site, service, or application is used primarily for K–12 school purposes and was designed and marketed for K–12 school purposes.

(b) An operator shall not knowingly engage in any of the following activities with respect to their site, service, or application:

(1) (A) Engage in targeted advertising on the operator's site, service, or application, or

(B) Target advertising on any other site, service, or application when the targeting of the advertising is based upon any information, including covered information and persistent unique identifiers, that the operator has acquired because of the use of that operator's site, service, or application described in subdivision (a).

(2) Use information, including persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a K–12 student except in furtherance of K–12 school purposes.

(3) Sell a student's information, including covered information. This prohibition does not apply to the purchase, merger, or other type of acquisition of an operator by another entity, provided that the operator or successor entity continues to be subject to the provisions of this section with respect to previously acquired student information.

(4) Disclose covered information unless the disclosure is made:

(A) In furtherance of the K–12 purpose of the site, service, or application, provided the recipient of the covered information disclosed pursuant to this subparagraph:

(i) Shall not further disclose the information unless done to allow or improve operability and functionality within that student's classroom or school; and

(ii) Is legally required to comply with subdivision (d);

(B) To ensure legal and regulatory compliance;

(C) To respond to or participate in judicial process;

(D) To protect the safety of users or others or security of the site; or

(E) To a service provider, provided the operator contractually (i) prohibits the service provider from using any covered information for any purpose other than providing the contracted service to, or on behalf of, the operator, (ii) prohibits the service provider from disclosing any covered information provided by the operator with subsequent third parties, and (iii) requires the service provider to implement and maintain reasonable security procedures and practices as provided in subdivision (d).

(c) Nothing in subdivision (b) shall be construed to prohibit the operator's use of information for maintaining, developing, supporting, improving, or diagnosing the operator's site, service, or application.

(d) An operator shall:

(1) Implement and maintain reasonable security procedures and practices appropriate to the nature of the covered information, and protect that information from unauthorized access, destruction, use, modification, or disclosure.

(2) Delete a student's covered information if the school or district requests deletion of data under the control of the school or district.

(e) Notwithstanding paragraph (4) of subdivision (b), an operator may disclose covered information of a student, as long as paragraphs (1) to (3), inclusive, of subdivision (b) are not violated, under the following circumstances:

(1) 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 protecting and disclosing that information.

(2) For legitimate research purposes: (A) as required by state or federal law and subject to the restrictions under applicable state and federal law or (B) as allowed by state or federal law and under the direction of a school, school district, or state department of education, if no covered information is used for any purpose in furtherance of advertising or to amass a profile on the student for purposes other than K–12 school purposes.

(3) To a state or local educational agency, including schools and school districts, for K–12 school purposes, as permitted by state or federal law.

(f) Nothing in this section prohibits an operator from using deidentified student covered information as follows:

(1) Within the operator's site, service, or application or other sites, services, or applications owned by the operator to improve educational products.

(2) To demonstrate the effectiveness of the operator's products or services, including in their marketing.

(g) Nothing in this section prohibits an operator from sharing aggregated deidentified student covered information for the development and improvement of educational sites, services, or applications.

(h) "Online service" includes cloud computing services, which must comply with this section if they otherwise meet the definition of an operator.

(i) "Covered information" means personally identifiable information or materials, in any media or format that meets any of the following:

(1) Is created or provided by a student, or the student's parent or legal guardian, to an operator in the course of the student's, parent's, or legal guardian's use of the operator's site, service, or application for K–12 school purposes.

(2) Is created or provided by an employee or agent of the K–12 school, school district, local education agency, or county office of education, to an operator.

(3) Is gathered by an operator through the operation of a site, service, or application described in subdivision (a) and is descriptive of a student or otherwise identifies a student, including, but not limited to, information in the student's educational record or email, first and last name, home address, telephone number, email address, or other information that allows physical or online contact, discipline records, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security number, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, or geolocation information.

(j) "K–12 school purposes" means purposes that customarily take place at the direction of the K–12 school, teacher, or school district or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school.

(k) 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.

(l) This section does not limit the ability of an operator to use student data, including covered information, for adaptive learning or customized student learning purposes.

(m) This section does not apply to general audience Internet Web sites, general audience online services, general audience online applications, or general audience mobile applications, even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications.

(n) This section does not limit Internet service providers from providing Internet connectivity to schools or students and their families.

(o) This section shall not be construed to prohibit an operator of an Internet Web site, online service, online application, or mobile application from marketing educational products directly to parents so long as the marketing did not result from the use of covered information obtained by the operator through the provision of services covered under this section.

(p) This section does not impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance of this section on those applications or software.

(q) This section does not impose a duty upon a provider of an interactive computer service, as defined in Section 230 of Title 47 of the United States Code, to review or enforce compliance with this section by third-party content providers.

(r) This section does not impede the ability of students to download, export, or otherwise save or maintain their own student created data or documents.

22585. This chapter shall become operative on January 1, 2016.

End Notes

[1] Software & Information Industry Association, Education Technology Industry Network, *SIIA Estimates $8.38 Billion US Market for PreK-12 Educational Software and Digital Content,* February 24, 2015, at *http://www.siia.net/Press/SIIA-Estimates-838-Billion-Dollars-US-Market-for-PreK-12-Educational-Software-and-Digital-Content*.

[2] ConnectED Initiative, at *https://www.whitehouse.gov/issues/education/k-12/connected*.

[3] U.S. Department of Education, Office of Education Technology, *Future Ready Learning: Reimagining the Role of Technology in Education*, 2016 National Education Technology Plan, January 2016,
p. 5, at *http://tech.ed.gov/netp/*.

[4] SIIA, 2014 U.S. Education Technology Market PreK-12, Executive Summary, at *http://www.siia.net/Portals/0/pdf/Education/SIIA2014Report_PreK12_FINAL%201%2031%202015_Exec%20Summ.pdf.*

[5] Monica Bulger, "Personalized Learning: The Conversations We're Not Having," 7/22/16, Data & Society Research Institute, *http://datasociety.net/.*

[6] Adam Newman, "Learning to Adapt: A Case for Accelerating Adaptive Learning in Higher Education," April 15, 2013, at *http://tytonpartners.com/library/accelerating-adaptive-learning-in-higher-education/*

[7] U.S. Department of Education, *loc. cit.*

[8] *www.oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-1685-million-settlement-k12-inc.*

[9] Otha Thornton, President, National PTA, quoted in *Leading K-12 School Service Providers Announce Pledge to Advance Student Data Privacy Protection,* October 7, 2014, at *www.pta.org/newsevents/newsdetail.cfm?ItemNumber=4260*

[10] Joel Reidenberg et al., *Privacy and Cloud Computing in Public Schools,* 2013, Center on Law and Information Policy. Book 2. *http://ir.lawnet.fordham.edu/clip/2.*

[11] U.S. Department of Education, "Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices," *http://ptac.ed.gov/*.

[12] *Ibid*.

[13] Common Sense Media, Protect Students" Data: Schools Must Be Privacy Zones, *https://www.commonsensemedia.org/kids-action/our-issues/a-positive-media-and-technology-world/school-privacy-zone.*

[14] The Future of Privacy Forum and The Software & Information Industry Association, Student Privacy Pledge, *www.studentprivacypledge.org*.

[15] 20 U.S. Code section 1232g.

[16] 20 U.S. Code section 1232h.

[17] No Child Left Behind Act, Sec. 1061: Student Privacy, Parental Access to Information, and Administration of Certain Physical Examinations to Minors, at *www2.ed.gov/policy/gen/guid/fpco/hottopics/ht04-10-02.html*.

[18] Privacy Technical Assistance Center, U.S. Department of Education, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, at *http://ptac.ed.gov/*.

[19] See *Owasso Independent School Dist. No. 1-011 v. Falvo, 534 U.S. 426 (2002)*, at *https://supreme.justia.com/cases/federal/us/534/426/case.html*, and Stephanie Simon, "Are Student Files Private? It Depends," *Politico*, May 15, 2014, *www.politico.com/story/2014/05/student-file-privacy-beyond-the-nsa-106687*.

[20] *See* Lynn M. Daggett, *FERPA in the Twenty-First Century: Failure to Effectively Regulate Privacy for All Students*, 58 CATH. U. L. REV. 59, 67 (2008), at *http://scholarship.law.edu/lawreview/vol58/iss1/*.

[21] 15 U.S. Code §§ 6501 et seq.

[22] FTC, Complying with COPPA: Frequently Asked Questions (March 2015), at *www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Schools*.

[23] AB 2799, Chapter 620 of the Statutes of 2016, enacted the Early Learning Personal Information Privacy Act (ELPIPA), Cal. Bus. & Prof. Code § 22586 *et seq.*, effective July 1, 2017.

[24] Cal. Ed. Code § 49073.1, included in Appendices.

[25] Cal. Bus. & Prof. Code § 22584 et seq. Also see Benjamin Herold, *'Landmark' Student-Data Privacy Law Enacted in California*, EDUCATION WEEK, September 30, 2014, at *http://blogs.edweek.org/edweek/DigitalEducation/2014/09/_landmark_student-data-privacy.html* and Maritza Jean-Louis, *California Breaks New Ground in Education Privacy Law with K-12 Student Data Privacy Bill, PROSKAUER PRIVACY LAW BLOG, September 17, 2004*, at *http://privacylaw.proskauer.com/2014/09/articles/california/california-breaks-new-ground-in-education-privacy-law-with-k-12-student-data-privacy-bill/*.

[26] Amelia Vance, "Data Privacy Laws Follow Lead of Oklahoma and California," *State Education Standard* 16, no. 2 (May 2016), p. 26, available at *www.nasbe.org*. For the latest information on state student data privacy laws, see the National Conference of State Legislatures, at *www.ncsl.org/research/education/student-data-privacy.aspx*.

[27] "Covered information" is defined at Cal. Bus. & Prof. Code § 22584 (i).

[28] See *supra*, Note 23. ELPIPA uses the term "pupil," where SOPIPA uses "student" and "preschool or kindergarten" where SOPIPA uses "school." In these recommendations, the use of "student" and "school" should be understood to include "pupil" and "preschool or kindergarten."

[29] See Cal. Ed. Code § 49073.1(7)(A) requiring contracts between educational agencies and Ed Tech companies to include a certification that pupil records shall not be retained or available to the company upon completion of the terms of the contract.

[30] U.S. Department of Education, *Data De-identification: An Overview of Basic Terms*, at *http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf*. National Center for Education Statistics, Institute of Education Sciences, *Statistical Methods for Protecting Personally Identifiable information in Aggregate Reporting*, December 2010, at *http://nces.ed.gov/pubs2011/2011603.pdf*, and *Basic concepts and Definitions for Privacy and Confidentiality in Student Education Records*, November 2010, at *http://nces.ed.gov/pubs2011/2011601.pdf*. Future of Privacy Forum. *De-Identification and Student Data*, *https://fpf.org/wp-content/uploads/FPF-DeID-FINAL-7242015jp.pdf*.

[31] Cal. Bus. & Prof. Code § 22584(b)4)(A) also requires that disclosures of covered information in furtherance of K-12 school purposes may be done only "to allow or improve operability and functionality within that student's classroom or school."

[32] Cal. Ed. Code § 49073.1(a)(6) requires school contracts for Ed Tech to contain a description of the procedures for notifying affected parents, guardians or eligible pupils of an unauthorized disclosure of *any information* directly related to a pupil that is maintained by the educational agency or acquired from the pupil through the use of Ed Tech. In addition, the data breach notification law, Cal. Civ. Code § 1798.29 (applies to state and local government agencies) and § 1798.82 (applies to businesses), requires notification of affected individuals of the unauthorized acquisition of certain categories of personal information, as defined. See also, for example, Cal. Civ. Code §§ 1798.80-1798.81 on disposal of customer records and 1798.81.5 on information security.

[33] See *Supra*, Note 30, for guidance on aggregation and de-identification of student data.

[34] See also Cal. Bus. & Prof. Code § 22581, which requires operators of sites and services directed to minors (under age 18) to provide a notice to minors who are registered users of the right to remove content or information posted on the site by the registered user.

[35] See the discussion of reasonable security in the Attorney General's *California Data Breach Report* (February 2016, at *www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf?*, and the Center for Internet Security, *The CIS Critical Security Controls for Effective Cyber Defense,* Version 6.0, October 2015, at *www.cisecurity.org*.

[36] FTC, *Start with Security: A Guide for Business*, available at *www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf*

[37] See *Supra*, Note 32.

[38] In addition to SOPIPA, see also the California Online Privacy Protection Act (Cal. Bus. & Prof. Code § 22575 et seq.), which requires disclosures regarding any personally identifiable information, as defined, collected by the operator of a commercial website or online service.

[39] See the Center for Information Policy Leadership, *Ten Steps to Develop a Multilayered Privacy Notice (2007)*, at *www.informationpolicycentre.com*.

[40] See *Supra*, Note 38.