National School Boards Association
cosa
Council of School Attorneys

Advising Schools on Digital Platforms: Privacy, Liability, and School District Bargaining Power

Mark Williams, Fagen Friedman & Fulfrost, Oakland, California

Presented at the 2017 School Law Practice Seminar, October 19-21, Chicago, IL

A PROPOSAL FOR THE ESTABLISHMENT OF A NATIONAL DATA PRIVACY AGREEMENT

By: Mark S. Williams

Introduction: This article will recount the increasing importance of technology in our economy and in digital products in our schools. Unfortunately, the system of contracting and procurement of digital products by school districts has not kept up with these rapid changes. Procurement is still largely fragmented – a consequence of individual state laws and under funding. It will be our thesis that this fragmentation can be overcome by the adoption of a Model Agreement that reflects the hidden commonalities of state statutes, and could be used on a nationwide basis. We propose a variant of the California Student Data Privacy Agreement ("CSDPA"), which is being used currently in California. We believe the CSDPA could be one of several documents that could establish a national system of student data privacy contracting and provide a cornerstone for a new national practice in student data privacy law, (and indeed for digital procurement generally), for education law practitioners.

Our Digital World. Technology has transformed virtually every aspect of our lives and at a hurtling pace. To cite one example, the list of the world's ten largest companies in 2007 contains only one technology company. The rest were almost all oil companies or banks.[1] In ten years, this list had been turned completely on its head. The four top spots are now occupied by technology companies (e.g., Apple, Alphabet, and Microsoft), with Amazon and China Mobile also taking spots in the Top 10.[2] In this same time period, entire new industries and fields of work have arisen and flourished, including such exotica as Data Analytics, Artificial Intelligence, Assisted Reality and Neural Networks. All of these companies and occupations are struggling to analyze and utilize a mind-boggling increase in data. It has been estimated that the total amount of stored data doubles every 24 months, a challenging companion to Moore's Law. In fact, by 2020 there will be an estimated 44 trillion gigabytes of stored data.[3]

Our Digital Schools. Education has also been transformed by technology. Last year school districts bought 8.9 million personal devices. Every school day 30,000 new Chromebooks are being activated in classrooms.[4] Most of the Common Core Standards are premised on the idea that students have access to personal devices and the internet.

---

[1] World's Largest Companies: 2016 vs 2006, Barry Ritholtz, http://ritholtz.com/2016/09/largest-companies-2016/, September 26, 2016.
[2] Id.
[3] The Exponential Growth of Data, Editorial Team, https://insidebigdata.com/2017/02/16/the-exponential-growth-of-data/, February 16, 2017 and 'Big Data' Is No Longer Enough: It's Now All About 'Fast Data', Tx Zhuo, https://www.entrepreneur.com/article/273561, May 13, 2016.
[4] Google's Chromebooks make up half of US classroom devices sold, Harriet Taylor, https://www.cnbc.com/2015/12/03/googles-chromebooks-make-up-half-of-us-classroom-devices.html, December 3, 2015, updated December 9, 2015.

continued…

Educators have mostly embraced digital learning. In one recent survey, 71% of the polled teachers saw themselves as "risk takers" or "early adopters" of digital education products. In addition, teachers have a high degree of confidence in the performance of educational digital products, with 70% of the polled teachers expressing "very high" or "high" confidence in their performance.[5]

However, a cautionary wind also blows around this confidence. When teachers are asked about their confidence in their school district's funding of technology, (which includes purchases and training), the numbers plunge to a mere 9%. Teacher confidence in effective policy making in digital education is not much higher, with 46% having little or no confidence in their district's ability to provide effective rules and guidance. The lack of funding and policy making may be part of the reason why the deployment of digital education in the classroom appears to be stuck in a lower gear, with many digital exercises restricted to rote learning or supplementing traditional lesson plans instead of instituting a system of interactive digital learning.[6]

Negotiating Technology Agreements. A lack of funding and effective public agency policymaking have plagued educators and school attorneys. This is particularly so in the procurement of digital products that store or utilize pupil records subject to The Family Educational Rights and Privacy Act ("FERPA"), or other state privacy laws. Primarily because of the expense involved, many school districts simply forego legal counsel entirely when reviewing and approving technology agreements. They are essentially hoping for the best, sometimes using lists of approved vendors supplied by other school districts.

When school attorneys are involved, technology procurements are often the result of "one off" contract negotiations between underfunded school districts and technology companies. Technology companies have carefully drafted their privacy language and other terms to cover general consumer uses outside of the FERPA structure, and are often even influenced by the language and terms of European Union treaties. Because of the concerns of consistency and interlocking legal obligations, technology vendors are reluctant to modify their agreements to suit the particular needs of a school district, however well-founded the proposed modification may be. Technology vendors have a real concern that any balkanization of "contract terms" will result in increased costs of administration and raises the danger of unintended consequences. In the face of vendor reluctance and the legal expenses of negotiation, many school districts swallow hard and sign agreements that have not been legally reviewed. Some districts utilize "bootlegged" acceptable vendor lists prepared by more experienced districts who may have legally vetted the products. Therefore, it is fair to say that the atmosphere surrounding school digital procurement is unsettled and tentative.

State Responses to Student Privacy. The last three years have witnessed an explosion of state legislation regulating the storage and use of student records. In 2016, 34 states introduced 112

[5] Teachers Still Struggling to Use Tech to Transform Instruction, Survey Finds, Anthony Rebora, http://www.edweek.org/ew/articles/2016/06/09/teachers-still-struggling-to-use-tech-to.html, June 6, 2016

[6] Id.

continued…

bills addressing student data privacy. Of this amount, 15 states passed 18 new student data privacy law.[7] So far in 2017, 13 states have bills pending addressing student data privacy.

These new laws are important to each state because they reflect a growing and nationwide intention to strengthen student data privacy, beyond the current protections given to it by federal statutes such as FERPA and the Children's Online Privacy Protection Act ("COPPA"). However, the proliferation of hundreds of state based statutes has the potential of further frustrating efforts to provide a method for economical contract negotiations and generally accepted contract forms. Before the explosion of state law addressing "ed tech" and student privacy, technology vendors could choose to negotiate with those relatively few school districts who sought a modification specific to the needs of their district.

Under the new statutes, technology contracts might have to be modified on a state-by-state basis, to meet the different requirements of each state law. As far as we can tell, technology vendors have not customized their products to meet the requirements of state laws. There is, as far as we know, no "Microsoft" or "North Carolina" version. Instead, the dangers of digital contract balkanization could actually strengthen from the passage of different state laws.

It is the height of irony that we find ourselves in a world where digital education products, which can store student data on cloud networks that cross national boundaries and connect students and educators to people and experiences on a global basis, are based on contracts whose scope extends only a few hundred miles. A product without borders requires a system of contracting that can at least cross some borders.

Efforts to Categorize and Standardize Digital Education. A number of individuals, companies and organizations have sought to organize and categorize student data and student data privacy agreements. For example, the Future of Privacy Forum ("FPF") maintains a database of all state privacy legislation. A4L is an international advocate for the Schools Interoperability Framework ("SIF") which sets standard categorizations of student data. The Student Data Privacy Consortium ("SDPC") is an alliance of a number of state agencies and school districts that maintains a registry of contracts, sorted by state, which complies with that state's privacy laws. Almost all of the contracts found on the Registry are "form" contracts that have been approved by legal counsel. School districts finding a contract formed within their own state can be reasonably certain that the vendors listed will enter into the same agreement with them for privacy purposes. However, the Registry is by state. Districts from other states could not be certain that the form agreement from another state would comply with their own laws.

CETPA and the CSDPA. The California Educational Technology Professionals Association ("CETPA") joined the SDPC in 2015 and began working on a CSDPA that would serve as a model agreement for school districts throughout the state. It was drafted by a number of authors, including this writer, Dana Greenspan and Steve Carr at the Ventura County Office of Education, and Michele Bowling, who is now a student at the Georgetown University School of Law's program in Cybersecurity and Data Privacy. The CSDPA has been vetted and approved by 69

[7] Student Data Privacy Legislation, Data Quality Campaign, http://dataqualitycampaign.org/wp-content/uploads/2016/09/DQC-Legislative-summary-09302016.pdf, September 2016.

technology companies including Clever, which was an early adopter of the Agreement and provided crucial feedback to help form a final CSDPA.

The Advantages and Challenges of a Model Agreement. This success of the CSDPA leads to a larger question: Could the CSDPA or another similar agreement serve as a model for a Uniform Student Data Privacy Agreement ("USDPA") that would be applicable everywhere in the country? The benefits of a USDPA would, of course, be immense. School districts and education lawyers would not be burdened with endlessly negotiating over the privacy provisions, and could focus on the other terms of the agreement, such as price warranties and product roll-out and training. For their part, vendors would have a unified and coherent legal agreement, thereby substantially reducing their costs and burdens. (A copy of a draft USDPA will be provided to participants at the time of the 2017 COSA School Law Practice Seminar.)

We believe there are three main challenges to the preparation and adoption of a USDPA. The first would be to determine whether a reconciliation of the differing state statues is even possible, given their number and different focuses. The second is that of "flexibility." Is it possible to draft a USDPA that would "fit all sizes," containing the required flexibility many vendors will demand, without undermining the "core" requirement of privacy statutes? Finally, there is the issue of "authentication." Determining whether any Model Agreement complies with all state laws is an ambitious enterprise and leaves room for error with a state-based practitioner who is unversed in the intricacies and relationships in the laws of another state.

Summary of Challenge Resolutions. We believe these three challenges can be resolved, as summarized below.

(i) <u>Differing State Statutes</u>:

We undertook a large scale study of other state student privacy laws, reviewing 22 in-depth. (By the time of the 2017 COSA School Law Practice Seminar, we expect to have reviewed the privacy laws of all 50 states.) We were searching to determine if there were common patterns in student data privacy laws and were there states where the CSDPA could extend. What we found surprised us.

We discovered that the hundreds of state student privacy statutes constitute a kind of "legal fractal," in which a seemingly complex set of separate legal enactments actually contain a large number of commonalities, and stem from a small set of organizing principles. We believe these commonalities can be summarized into three core organizing principles. First, in almost all of the state statutes, the FERPA requirements are expressly incorporated therein. A great deal has been written about the age of FERPA (it was passed in 1974) and how it was written before the advent of the personal computer or the internet. All of this true. Yet it has been a remarkably durable enactment, aided by straightforward regulations and well-thought-out advice by the Privacy Technical Assistance Center ("PTAC") in the Department of Education. PTAC has given FERPA fresh new meeting in emerging issues, such as data breach responses.

Many states have also passed legislation similar to California's two student privacy laws. The Student Online Personal Information Protection Act ("SOPIPA") (found at California's Business

and Professions Code section 22584) is itself a broadening of the protections found in the Children's Online Privacy Protection Act ("COPPA") found at 15 U.S.C.A. § 6501. The second statute has the popular name of AB 1584 (found at Education Code section 49073.1), and focuses on the required elements of school technology contracts. In other words, most of the new state statutes can be traced back to a small set of antecedent legislation, particularly FERPA the "Ur" law of student data privacy.

Secondly, the statutes raise a relatively limited number of issues about student data privacy and resolve them almost always in the same way, reflecting an underlying political and social consensus on the treatment of student data. For example, no state allows student records to be sold on the open market; and it is reasonable to assume that no state would allow such a practice.

In some cases, there are substantive differences, but for the most part, the subject matters of the differences lie on the periphery or beyond the rules controlling the heart of most technology vendor agreements. For example, a number of states have enacted statutes that govern the formation of state databases and the information they will receive from school districts. Other states regulate cross-state flows of information pursuant to the "Educational Opportunity for Military Children Compact." A few states do admittedly have some substantive differences. However, we believe the legal requirement of these few states could be addressed by specific "riders" to the USDPA.

(ii) USDPA Flexibility. The second challenge relates to the required flexibility of any Model Agreement. We have found that the CSDPA (the document upon which the USDPA is based), has been surprisingly flexible in addressing the specific requirements and requests of particular vendors. For example, many vendors wish to add the details of their data security plans to the more general requirements found in the USDPA. Their requests are easily accommodated because they do not alter the Agreement's underlying minimum security requirements. To the contrary, vendor security plans describe procedures and measures that exceed , strengthen and/or supplement state or recognized technical standards.

Parties to a particular Agreement may need to add amendments to the USDPA to accurately reflect, among other things, complex exchanges of student records between groups of school districts, research institutions and independently operating academics. All of them may have one goal, the improvement of student performance for example, but their tasks will vary and take place in wildly different settings.

(iii) The Issue of Authenticity. Finally, there is the issue of authenticity. How will we know for certain that a USDPA is and remains applicable in all of the states? In a world of underfunding, we suggest the adoption of the digital "crowd sourcing." School attorneys in particular states are asked to provide insight as to whether the draft USDPA conforms with their law and it if does not, what modifications might be required. In return, all participants will have an available "open source" and usable agreement for their own needs.

1. The Common Sources of Student Data Privacy Law

Much of student data privacy laws are conceived from two sets of legislation. At the federal level, there is FERPA and COPPA. At the state level, California's AB 1584 and SOPIPA have also been influential. The key provisions of these four laws overlap and can be organized under two concepts. First, each piece of legislation focuses on a different aspect of a data transfer transaction. Second, the California legislation either expands or amplifies FERPA and COPPA, while adding the element of data security.

FERPA and AB 1584. FERPA is, of course, the "Ur" student data privacy legislation. Most subsequent legislation, whether at the federal level or the state level, reflects its rules and values to some degree. FERPA focuses on school districts, and makes compliance with the Act a condition for receiving education funds.[8] FERPA protects and regulates the disclosure of education records, a term defined to include information "directly related to a student" and "maintained by an educational agency or institution or by a party acting for such agency or institution."[9]

As it pertains to third party vendors, school districts may disclose non-directory education records in one of two ways. First, they may do so with the consent of the student's parents.[10] Alternatively, education records may be disclosed to third parties under the "school official" exception. A vendor may be considered a school official if the vendor: (i) performs an institutional service or function for which the institution would otherwise use employees; (ii) is under the direct control of the institution with respect to the maintenance of education records; and (iii) is subject to certain FERPA requirements regarding the use of the education records.[11] This includes using the education record for the purposes for which the disclosure is made.[12]

AB 1584 has a narrower focus than FERPA. It shifts the focus of legal scrutiny away from school districts to the contracts between school districts and third party vendors. It sets out the subjects that must be addressed in a technology contract. The "teeth" of enforcement is not a cutoff of education funds, but the voiding of the non-compliant contract.[13] AB 1584 does not contradict or substantially modify FERPA duties; it simply provides more specificity and adds two topics that may be implied from the FERPA statute. Interestingly, AB 1584 calls the protected data "pupil records" rather than "education records," the first of many variances in the naming of student data.

AB 1584 requires that school district-third party tech contracts contain:

1. A statement that the pupil records continue to be the property of and under the control of the school district;

[8] 20 U.S.C.A. § 1232 (g) (1) (A)
[9] 20 U.S.C.A. § 1232g(a)(4)
[10] 20 U.S.C.A. § 1232g(b)(2)
[11] 34 C.F.R. § 99.31 (a)(1)(i)(B)
[12] 34 C.F.R. § 99.33(a)
[13] Cal. Educ. Code § 49073.1 (c)

2. A description of the means by which pupils may retain possession and control of their own pupil generated content, 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 student'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;
6. A description of the procedures for notifying the affected parent, legal guardian or eligible pupil in the event of an unauthorized disclosure of the pupil's records;
7. A certification that a pupil's records shall not be retained or available to the third party upon completion of the terms of the contract and a description of how that certification will be enforced;
8. A description of how the local education agency and the third party will jointly ensure compliance with FERPA; and
9. A prohibition against the third party using personally identifiable information in the pupil records to engage in targeted advertising.[14]

AB 1584 also states that the identified information does not fall within the definition of pupil records and may be used by the third party vendor to: (i) provide adaptive learning and customizing pupil learning; (ii) demonstrate the effectiveness of the vendor's products; and (iii) improve the vendors' sites, services, or applications.[15]

It can be argued that AB 1584's main substantive addition to FERPA is the explicit requirement for a data security plan and notification in the event of unauthorized access to pupil records. As privacy laws develop and the threat of cyber breaches grows, these substantive additions may be the most important elements in any privacy agreements and the section most open to modification and debate.

COPPA and SOPIPA. Unlike FERPA and AB 1584, COPPA does <u>not</u> presume the presence of a school district in a data transaction. Its fundamental focus instead is on the relationship between websites and on-line services geared to children and the parents of children using a website or service. One of the main determinants of that relationship is the presence or absence of parental consent. With parental consent, an operator may collect, use and disclose personal information.[16] However, even with parental consent, the operator must establish reasonable procedures to protect the confidentiality, security, and integrity of personal information.[17]

[14] Cal. Educ. Code § 49073.1 (a)
[15] Cal. Educ. Code § 49073.1 (c) (5) (B)
[16] 15 U.S.C.A. § 6502 (b) (1)
[17] 15 U.S.C.A. § 6502 (d)

Although SOPIPA is substantially related to COPPA, it greatly expands its scope and requirements. Like COPPA, SOPIPA also does not generally presume the presence of a school district. More importantly, it does not focus on the relationship of a parent and an operator and the accompanying issue of consent. Its rules apply even in the absence of parental consent. It establishes "rules of the road" for operators that automatically apply to an operator's product that is used primarily for K-12 school purposes and was designed and marketed for K-12 school purposes. Unlike COPPA, it applies to children 13 and older, and includes non-profit as well for profit operators. It does not presume a contract.

SOPIPA can be compared to AB 1584 with two observations. First, SOPIPA does not appear to be based on the school official exception; the educational duties found in AB 1584, such as the modification of student records, or the creation of separate student accounts are absent from the Act. Second, SOPIPA provides more specificity as to what acts constitute an unauthorized use of "covered information." Operators must not sell covered information, create profiles unrelated to the educational use of the information, or engage in targeted advertising.

2. The Purpose and Elements of the CSDPA

We have attached the CSDPA, the document we propose as the prototype for a national model, for review and comment. The CSDPA was designed to accomplish three objectives: (1) to provide a means of compliance with the main student data privacy statutes such as FERPA and AB 1584; (2) to address some of the social and cultural issues posed by digital education and the use of outside vendors to perform school functions; and (3) to address, in a practical and balanced way, the technical issues that may arise in the operation of digital services and products in a variety of settings. Let's walk through it and see how it works.

Article 1 – Provides an overview of the data transaction between the school district and the vendor. Sections 1 and 2 describe the purpose of the data transfer and the data to be transferred. We believed it was vital to "front load" these elements. Many vendor contracts bury the underlying purpose of the contract behind a bundle of licensing and warranty terms. Members of the public and even Board members are mystified when reading the terms of these traditional agreements. The CSDPA provides two of the three vital elements many parents consider when assessing the transfer of the child's personal data: What information are we giving up and what are we getting in return? [18]

Article II – Sets out most of the basic duties of FERPA and AB 1584. The reader will note that the vendor does not have the "primary" duty to modify student records or to create a separate account. They are left to the ministerial duty of allowing or executing instructions given to a local educational agency ("LEA"). We believe this secondary role reflects larger legal duties and administrative realities.

Article III – Establishes some duties of the school district regarding the contract. For the effective execution of a data privacy agreement, we believe there should be active engagement by the school district. It also builds vendor confidence that the CSDPA is balanced.

[18] In our experience, the third element of parent concern is data security.

Article IV – Establishes additional responsibilities and sets out additional duties. Most notably, it sets out alternatives by which student data may be disposed of at the end of the contract term.

Article V – Data Security and Breach Notification: This section was the one most open to flexibility. It tries to bridge the need for specificity with the knowledge that cutting-edge practices can be quickly outpaced by technological advancements. (For example, the designation of Secure Socket Layer in subsection (e), may soon be outmoded.) We therefore did a mix of general practices tied to NIST 800-63-3. Future editions can revise this section to retain its relevance.

Article VI – This Article provides a "General Offer" to all other school districts. If the vendor signs the Exhibit "E" to the CSDPA, the vendor agrees to be bound to the same privacy terms with any other school district for contracts entered into within three years of signature. In other words, if the CSDPA conforms to the laws of other states, this General Offer applies to districts in those states. (Most of the vendors signing the CSDPA have also signed the General Offer.)

Article VII – A priority of Agreements is found in this Article. In the event there is a conflict between the privacy terms of the vendor service agreement and the CSDPA, the CSDPA prevails.[19]

The CSDPA has been signed by 70 companies and used by dozens of school districts in California. The question then becomes, can it, or a variant of it, be used in other states? We provide some analysis of this issue below. We believe the answer is "yes."

3. An Examination of State Student Data Privacy Laws

Let us examine the Data Privacy laws of five states to determine whether they are consistent with SOPIPA, and AB 1584, thereby allowing the use of the CSDPA in those jurisdictions. There was no scientific schema employed in the selection of the five states; we used such factors as size and region. Prior to our review, we had not been apprised of any unique factors to the laws of these states. Therefore, these five states may serve as a base line for finding a general rule.

(a) Arizona. The focus of Arizona student data privacy laws has been, until recently, the establishment and regulation of a State Department of Education database, which specifies the kinds of data to be submitted to the database, and the uses to which the data may be put.[20] The

[19] Oddly enough, many vendor contracts downplay the security measures undertaken by the company, which are often comprehensive and world class. The GAFE contract documents are a classic example.

[20] It is a persistent habit of many vendors to insert into their service agreements provisions to the effect that their privacy policies, found online can change, with or without notice to the customer. This language puts at risk the protections of FERPA and SOPIPA .

continued…

statute specifically requires the Department of Education to comply with FERPA in the disclosure of any student data collected.[21] Specific responsibilities include:

- "Proper security measures are employed to ensure the confidentiality and integrity of the education database.

- Data is secured from breaches and identity theft through the implementation of protections and standards."[22]

Arizona has also entered into the Interstate Compact on Educational Opportunities for Military Children. Among other things, the Compact defines "educational records" and provides for the uniform collection and sharing of information between and among member states, schools, and military families as children move from state to state.[23]

Arizona passed a flurry of student privacy bills during the 2017 legislative session. Senate Bill 1098 requires the State Board to implement a statewide assessment to measure pupil achievement in the State. The State Board also must survey teachers, principals and superintendents on achievement related to non-test indicators, including information on graduation and dropout rates by ethnicity. In conducting this survey, the State Board cannot violate the provisions of FERPA, nor disclose personally identifiable information.

More importantly, Arizona passed SB 1134 during its 2017 legislative session. SB 1134 adds Section 15-046 to the Education Code and is closely modeled after California's SOPIPA and includes the following:

1. Prohibits targeted advertising by the operator.
2. Prohibits an operator from creating a student profile, except in furtherance of educational purposes.
3. Prohibits an operator from selling or renting student information.
4. Requires and operator to maintain reasonable security measures and practices.
5. Binds operator-supported third party providers to the same duty of confidentiality. [24]

Arizona, therefore, has followed almost exactly the pattern of state Student Privacy law suggested earlier. Until recently, the legislative focus has been on establishing a State educational records database, and determining how the information to and from this database would, among other things, protect student privacy. FERPA was the quoted standard for student privacy. This changed recently with the adoption SB 1314. However, SB 1314 appears to be a

[21] Ariz. Rev. Stat. Ann. § 15-1041. A significant number of states more or less incorporate FERPA as the general standard by which education records will be protected. Examples include Alabama, Alaska, and Florida.
[22] Ariz. Rev. Stat. Ann. § 15-1045
[23] Ariz. Rev. Stat. Ann. § 15-1911
[24] Ariz. Rev. Stat. Ann. § 15-1046 (4) (f)

continued…

variant and extrapolation of the SOPIPA statute. Therefore, we believe that a SOPIPA complaint Model agreement would also comply with SB 1314.[25]

(b) Minnesota. Minnesota's statutes regulating Education Records (Minnesota terms Education Records "Education Data") are found in a comprehensive and well-organized group of statutes called Government Data Practices Act ("Act").[26] (The Act is 176 pages long.) Privacy protections for Education Data are found in two separate sections. The first set of applicable statutes are of general application, and apply to school districts as "Responsible Authorities."[27] As a Responsible Authority, Minnesota school districts must establish appropriate security safeguards for all records containing data on individuals and develop policies incorporating these procedures.[28] School districts may enter into contracts with private persons to perform any of their functions, but the contracts must state that they are subject to the requirements set forth in the Act.

The Act also contains a section addressing responses to data breaches, which is very similar to the data breach statutes found in California law.[29] This section prescribes the contents of the notice that a governmental agency must give to an affected individual, and how the notice may be given. The Notice must be made in the most expedient time possible and without unreasonable delay.[30] When the investigation of the data breach is completed, the agency must prepare a report describing the type of data accessed, the number of individuals affected, and the disciplinary action taken against an employee in the event the employee caused the breach.[31]

The Act also contains a set of sections specifically applicable to school districts.[32] However, these sections for the most part govern access to specified individuals and government agencies. They do not appear to be directly related to issues pertaining to contracts between school districts and third party vendors.

---

[25] It can be argued that Arizona SB 1314 has one very important difference from SOPIPA. Section (H) requires school districts to pass policies which will allow parents to "opt out" of technology products and the internet. Whatever the wisdom of that section is, it will have no direct bearing on district contracts with vendors, except in very limited circumstances (e.g., deletion of accounts and account information upon request of the District). Therefore, this section supports our theory that variances in the law lie at the periphery or beyond of the contents of a third party contract.

[26] Minn. Stat. Ann. § 13.01, et seq. Other states, seeking to establish their own data privacy laws, would do well to look to Minnesota's logical and clear statutory scheme, all contained in a single set of statutes. This author's state of California has a more fragmented approach, with student privacy laws contained in at least three different codes.

[27] Minn. Stat. Ann. § 13.02, Subd. 5 (2) and (3)

[28] Minn. Stat. Ann. § 13.05

[29] Minn. Stat. Ann. § 13.055 The California cites are Civil Code sections 1798.29 (government agency) and 1798.80 (business).

[30] Minn. Stat. Ann. § 13.055 Subd. 2.

[31] Minn. Stat. Ann. § 13.055 Subd. 2.

[32] Minn. Stat. Ann. § 13.319 to 13.322

continued…

Minnesota's laws regarding data security, data breach response, and school district contracting are consistent with the provisions of CSDPA and the statutes of most of the other states that have addressed these issues. A USDPA could be devised that is applicable in Minnesota.

(c) Maryland. Maryland's statutory structure regarding the privacy of student Education Records is relatively consistent with those of the states surveyed. Education Records are divided into two groups: (1) Covered information, which has a comprehensive meaning; and (2) Student data, which appears to be limited to records of student achievement, such as state and national assessments, grades and grade point average.[33] Like many other states, Maryland has implementing statutes for the Interstate Compact on Educational Opportunity for Military Children. It has also established a statewide database called the Maryland Longitudinal Data System Center.[34]

Md. Code Ann., Educ. § 4-131 incorporates most of the rules pertaining to the use of Education Records by third party vendors. In this statute, Maryland has taken a creative and commendable approach to bridging the "legal gap" between FERPA and COPPA at the federal level, and such statutes as AB 1584 and SOPIPA at the state level. As it will be recalled, FERPA and AB 1584 focus on school districts and vendors in data transactions, FERPA through the school official exception and AB 1584 through the contents of data contracts. On the other hand, COPPA and SOPIPA do not presume such a contractual relationship and focuses instead on the relationships between vendors, students and the student's parents.

The problems arise when individual teachers wish to use education applications and sign the "click wrap" agreements. Does this satisfy the parent consent requirement of COPPA? On a broader level, does the teacher's signature take the application out of COPPA and SOPIPA entirely and convert it into a school official relationship or technology contract governed by FERPA and AB 1584 and other similar state statutes? The answer to the first question appears to have been answered recently by the Federal Trade Commission ("FTC"). The FTC has stated that a teacher can give consent on behalf of a parent for the purposes of COPPA.[35]

The second question is more troubling for many state practitioners. Under traditional rules of school district contracting, teachers acting on their own, cannot bind a school district to a contract. In most instances, they must be approved by the Board of Education. However, how does such a process work when a given school district needs to use dozens, or even hundreds of applications?

Maryland has come up with a practical answer. It has simply expanded the power of procurement for education apps. to individual teachers, [36] thereby bridging the gap between COPPA and FERPA . Maryland then lists the same requirements found in SOPIPA and AB

[33] Md. Code Ann., Educ. § 4-131 and 24-701
[34] Md. Code Ann., Educ. § 24-703
[35] FTC FAQ M.1, Mar 20,2015.
[36] Md. Code Ann., Educ. § 4-131(a)(3)

continued…

1584. For example, operators are prohibited from making student profiles except in furtherance of school purposes.[37] Service providers that provide functions to the operators are bound to the same privacy requirements of the operator. Operators may use aggregated or de-identified covered information to demonstrate the effectiveness of the operator's product and to improve the service.[38]

In other words, this creative statutory "bridging" employed by Maryland does not appear to detract the applicability of the CSDPA to services and products under Maryland law. The overall pattern holds.

(d) North Carolina. North Carolina passed a SOPIPA-based statute in 2016.[39] North Carolina's law closely tracks SOPIPA with a few exceptions. One of the main exceptions is a narrowing of the term "targeted advertising" to exclude offerings or recommendations within the site based on the student's use of the vendor's system.[40] This appears to be a significant weakening of the term "targeted advertising," and is an issue that should be examined closely to see if a modification to the CSDPA is necessary or whether a rider to the agreement is desired. Fortunately, nothing prevents a school district from contracting for a higher level of protection than that set by legislation. With this one caveat, North Carolina law aligns with SOPIPA and appears to be consistent with the terms of the CSDPA.

(e) Texas. On June 1, 2017, the Governor of Texas signed into law a version of SOPIPA, HB 2087. The wording of the statute mostly matches that found in SOPIPA. However, some of the language of the new law appears to be weaker than the language found in SOPIPA. For example, an operator can use or disclose the data for "legitimate research" unaccompanied by the arguably stricter protective language surrounding use of data for research. In addition, HB 2087 permits the operator to use data to demonstrate the effectiveness of an operator's product or to improve its service where the data is "not associated with an identified student."[41] The phrase "Not associated with a student" is not a defined phrase within the statute, but appears to lack the precision and level of information that has been "de-identified." A closer look at the legislative history may be in order.

Whatever the result, it does not appear that HB 2087 is stronger or substantially different from SOPIPA. Therefore, it would appear that the CSDPA would apply under Texas laws as well.

Conclusion: In the five states listed here, (and in the 15 or so other states we have reviewed and are not listed here), we have found a remarkable similarity in the state statutes surveyed. We believe that the CSDPA could, with minor variations, be deployed in these states. Practitioners may ponder how "targeted advertising" should be defined. However, since the CSDPA takes a

[37] Md. Code Ann., Educ. § 4-131 (d) (1) (ii)
[38] Md. Code Ann., Educ. § 4-131 (g)
[39] N. Car. stat 115c-401.2
[40] N. Car. stat 115c-401 (e) (4)
[41] Tex. stat. 32.154 (B)

stricter view than other states (i.e., no targeted advertising at all), it would certainly meet the arguably more relaxed advertising standards for some of the states surveyed.

4. Three "Exceptions": An Examination of Three States

It can be argued that although a USDPA could ~~not apply to~~ be used in most states, it possibly could not be used in those states that have adopted particularly unique rules. In those cases, an attachment to the USDPA might be required for use within that state only. To see whether this would in fact be required, we examined the laws in three states that have adopted a specialized set of rules: Colorado, Louisiana and New York.

(a) Colorado. In 2014, Colorado passed HB 14-1294, and in 2016, HB 16-1423, which made several significant changes to Colorado laws for student data privacy. The bulk of HB 14-1294 is providing direction to the Colorado Department of Education to protect data, including requiring Department contracts to safeguard privacy and security. It requires that the contract specify that personally identifiable data may only be used for the purposes specified in the contract and prohibit further disclosure of that data or its use for commercial purposes.[42]

HB 14-1294 also tasked the State Department of Education with preparing and making publicly available such resources as policies and procedures to comply with FERPA and other relevant privacy laws, and with developing a detailed data security plan.[43] However, there is little additional material that directly addresses vendor contracts with local school districts.

In contrast, HB 16-323 does have sections relating to the contracting procedures of local school districts, commencing at section 22-16-107. However, many of those sections relate to the duties of the school district to promote contracting transparency, by among other things posting technology contracts on its website and to provide a public hearing for vendors in the event there is a breach of the privacy provisions in a technology contract.[44] HB 16-323 has three sections regulating technology vendor contracts, which include provisions allowing for access and correction of erroneous student records, prohibiting the sale of student data, and requiring vendors to maintain comprehensive data security programs.[45]

Based on our review of the of HB 14-1294 and HB 16-1423, it appears that these two bills have added significantly to the duties of the Colorado Department of Education and school districts in terms of providing resources and public transparency. It does not appear to have altered the core requirements of AB 1584 or SOPIPA. As the Model is developed, the data security plan developed by the Colorado Department of Education should be scrutinized to see if any of its elements should be added to the security sections of the Model.

[42] Colo. Rev. Stat. Ann. § 22-2-309 (g)
[43] Colo. Rev. Stat. Ann. § 22-2-309 (3) (b) and (d)
[44] Colo. Rev. Stat. Ann. § 22-16-107 (2)
[45] Colo. Rev. Stat. Ann. § 22-16-108

continued…

(b) Louisiana. Louisiana statutes addressing the sharing of student data to third party vendors appear to be in a state of flux. In 2014, Louisiana passed HB 946, which prevented the sharing of student data to third parties without parental consent, except in narrow circumstances.[46] This was followed a year later by the passage of HB 719, which appears to ease the restrictions of HB 1283.

Under the new statute, student data can be shared with third party vendors, so long as the vendor does not use the data for unauthorized purposes.[47] Vendors also may not use the data for predictive modeling for the purpose of limiting the educational opportunities for students.[48] As we read the statute, we do not think Louisiana law sets up a significant challenge to third party digital contracts. Louisiana has caught the attention of the press because of its draconian penalties in the event an educator or vendor discloses student data in an unauthorized manner. In such a case the person can be subject to six months of imprisonment.

(c) New York. In many respects, New York follows the rules established by AB 1584, and the requirements of the CSDPA. For example, third party vendors must notify a school district if there has been unauthorized access to student data.[49] Vendors must use reasonable safeguards to protect the security, confidentiality and integrity of personally identifiable information.[50] Parents will have the right to inspect and review their child's records.[51]

However, our review of New York law in student data revealed a significant variance in at least three areas. First, there are very detailed security requirements for third party vendors. These security requirements include encryption technology that complies with technologies or methodologies established by the United States Department of Health Services for medical information.[52] The details of security practices can be varied under the CSDPA. However, in New York's case, the security language must mirror the specific standards of HIPPA. For this reason we recommend that a security amendment be adopted for contracts with New York school districts.

Second, parents are required to be told where student data will be stored.[53] This language presumes the use of a server. We think vendors who store student data in the cloud will have a difficult time meeting this requirement. The vendor should be consulted regarding this requirement.

[46] La. Stat. Ann. § 17:3914 (C) (2)
[47] La. Stat. Ann. § 17:3914 (3) (F) (2)
[48] La. Stat. Ann. § 17:3914 (G)
[49] New York Consolidated Laws, Education Law - EDN § 2-d 6
[50] New York Consolidated Laws, Education Law - EDN § 2-d 5 f (4)
[51] New York Consolidated Laws, Education Law - EDN § 2-d 3 b (2)
[52] New York Consolidated Laws, Education Law - EDN § 2-d 5 f (4)
[53] New York Consolidated Laws, Education Law - EDN § 2-d 3 c (4)

continued…

Finally, and perhaps most importantly, New York law requires each school district to adopt a "parent's Bill of Rights."[54] This Bill of Rights must be attached to each vendor contract.[55] This statutory language at least raises the possibility that data privacy restrictions may vary significantly from district to district, and carries further the threat of "procurement balkanization" discussed above.

Summary: As we read the laws of the three possible exceptions, it appears that only New York's law is significantly different in the area of third party contracts. School districts in New York using the CSDPA may be required to use an amendment.

5. Authenticity

As noted above, the last few years have witnessed an explosion in state legislation regarding student data privacy. If the CSDPA or another variant captures most of the state variations *now*, there may be room for uncertainty as to whether it will capture changes enacted by state law in the future. Education law practitioners should discuss ways to notify each other in the event that changes in the laws of their state challenge the applicability of the USDPA. COSA, SDPC or other suitable association could serve as an information clearinghouse. In this way, one of the challenges of a digital age could be met through the employment of a digital practice: crowdsourcing.

6. Conclusion

The end of World War II spurred an explosion in economic growth across state lines, including the construction of an interstate highway system. There was a need to standardize the laws of commercial transactions in a system where goods might be manufactured in one state, warehoused in another state and delivered to a third state. Thus was born the Uniform Commercial Code. As student information is increasingly stored and utilized in cloud systems that span states and countries, there is a similar need to standardize laws and contract terms. Perhaps the CSDPA can become one small piece in the answer to this challenge.

00618-00001/4099645.1

[54] New York Consolidated Laws, Education Law - EDN § 2-d 3
[55] New York Consolidated Laws, Education Law - EDN § 2-d 5 (e)

CALIFORNIA STUDENT DATA PRIVACY AGREEMENT

(July 10, 2017)

_____ School District

and

_____

[DATE OF SERVICE AGREEMENT]

This California Student Data Privacy Agreement ("DPA") is entered into by and between the _____ District (hereinafter referred to as "LEA") and _____, hereinafter referred to as "Provider") on [Insert Date]. The Parties agree to the terms as stated herein.

RECITALS

WHEREAS, the Provider has agreed to provide the Local Educational Agency ("LEA") with certain digital educational services ("Services") pursuant to a contract dated [Insert Date] ("Service Agreement"); and

WHEREAS, in order to provide the Services described in the Service Agreement, the Provider may receive and the LEA may provide documents or data that are covered by several federal and statutes, among them, the Family Educational Rights and Privacy Act of 1974 ("FERPA") at 12 U.S.C. 1232g, Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502; Protection of Pupil Rights Amendment ("PPRA") 20 U.S.C. 1232 h; and

WHEREAS, the documents and data transferred from California LEAs are also subject to several California student privacy laws, including AB 1584, found at California Education Code Section 49073.1 and the Student Online Personal Information Protection Act (sometimes referred to as either "SB 1177" or "SOPIPA") found at California Business and Professions Code section 22584; and

WHEREAS, the Parties wish to enter into this DPA to ensure that the Service Agreement conforms to the requirements of the privacy laws referred to above and to establish implementing procedures and duties; and

WHEREAS, the Provider may, by signing the "General Offer of Privacy Terms", agrees to allow other LEAs in California the opportunity to accept and enjoy the benefits of this DPA for the Services described herein, without the need to negotiate terms in a separate DPA.

NOW THEREFORE, for good and valuable consideration, the parties agree as follows:

ARTICLE I: PURPOSE AND SCOPE

1. **Purpose of DPA**. The purpose of this DPA is to describe the duties and responsibilities to protect student data transmitted to Provider from the LEA pursuant to the Service Agreement, including compliance with all applicable privacy statutes, including the FERPA, PPRA, COPPA, SB 177 (SOPIPA), and AB 1584. In performing these services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA. Control duties are set forth below.

2. **Nature of Services Provided**. The Provider has agreed to provide the following digital educational services described below and as may be further outlined in Exhibit "A" hereto:

[Insert Brief Description of Services]

3. **Student Data to Be Provided**. In order to perform the Services described in the Service Agreement, LEA shall provide the categories of data described below or as indicated in the Schedule of Data, attached hereto as Exhibit "B":

[Insert Categories of Student Data to be provided to the Provider]

4. **DPA Definitions**. The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over term used in the Service Agreement.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. **Student Data Property of LEA**. All Student Data or any other Pupil Records transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data or any other Pupil Records contemplated per the Service Agreement shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEAs as it pertains to the use of student data notwithstanding the above. Provider may transfer pupil-generated content to a separate account, according to the procedures set forth below.

2. **Parent Access**. LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information on the pupil's records, correct erroneous information, and procedures for the transfer of pupil-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner to the LEA's request for personally identifiable information in a pupil's records held by the Provider to view or correct as necessary. In the event that a parent of a pupil or other individual contacts the Provider to review any of the Pupil Records accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. **Separate Account**. Provider shall, at the request of the LEA, transfer Student generated content to a separate personal student account.

4. **Third Party Request**. Should a Third Party, including law enforcement and government entities, contact Provider with a request for data held by the Provider pursuant to the Services, the Provider shall redirect the Third Party to request the Student Data directly from the LEA. Provider shall notify the LEA in advance of a compelled disclosure to a Third Party unless legally prohibited.

5. **No Unauthorized Use**. Provider shall not use Student Data purposes other than as explicitly specified in the Service Agreement.

6. **Subprocessors**. Provider shall enter into written agreements with all Subprocessors performing functions pursuant to the Service Agreement, whereby the Subprocessors agree protect Student Data in manner consistent with the terms of this DPA

ARTICLE III: DUTIES OF LEA

1. **Provide Data In Compliance With FERPA**. LEA shall provide data for the purposes of the Service Agreement in compliance with the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. section 1232 g, AB 1584 and the other privacy statutes quoted in this DPA.

2. **Reasonable Precautions**. LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted data.

3. **Unauthorized Access Notification**. LEA shall notify Provider promptly of any known or suspected unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

4. **District Representative**. At request of Provider, LEA shall designate an employee or agent of the District as the District representative for the coordination and fulfillment of the duties of this DPA.

ARTICLE IV: DUTIES OF PROVIDER

1. **Privacy Compliance**. The Provider shall comply with all California and Federal laws and regulations pertaining to data privacy and security, including FERPA, COPPA, PPRA, AB 1584, and SOPIPA.

2. **Authorized Use**. The data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services stated in the Service Agreement and/or otherwise authorized under the statutes referred to in subsection (1), above.

3. **Employee Obligation**. Provider shall require all employees and agents who have access to Student Data to comply with all applicable provisions of FERPA laws with respect to the data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. **No Disclosure**. Provider shall not disclose any data obtained under the Service Agreement in a manner that could identify an individual student to any other entity in published results of studies as authorized by the Service Agreement. Deidentified information may be used by the vendor for the purposes of development and improvement of educational sites, services, or applications.

5. **Disposition of Data**. Provider shall dispose of all personally identifiable information ("PII") obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained and transfer said data to LEA or LEA's designee within 60 days of the date of termination and according to a schedule and procedure as the Parties may reasonably agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data obtained under the Service Agreement beyond the time period reasonably needed to complete the disposition. Disposition shall include (1) the shredding of any hard copies of any Pupil Records; (2) Erasing; or (3) Otherwise modifying the personal information in those records to make it unreadable or indecipherable. Provider shall provide written notification to LEA when the Data has been disposed. The duty to dispose of Student Data shall not extend to data that has been de-identified or placed in a separate Student account, pursuant to the other terms of the DPA.

6. **Advertising Prohibition**. Provider is prohibited from using Student Data to (a) market or advertise to students or families/guardians; (b) inform, influence, or enable marketing, advertising, or other commercial efforts by a Provider; or (c) develop a profile of a student, family member/guardian or group, for any commercial purpose other than providing the Service to Client.

ARTICLE V: DATA PROVISIONS

1. **Data Security**. The Provider agrees to abide by and maintain adequate data security measures to protect Student Data from unauthorized disclosure or acquisition by an unauthorized person. The general security duties of Provider are set forth below. Provider may further detail its security programs and measures in in Exhibit "D" hereto. These measures shall include, but are not limited to:

    a. **Passwords and Employee Access**. Provider shall make best efforts practices to secure usernames, passwords, and any other means of gaining access to the Services or to Student Data, at a level suggested by Article 4.3 of NIST 800-63-3. Provider shall only provide access to Student Data to employees or contractors that are performing the Services. As stated elsewhere in this DPA, employees with access to Student Data shall have signed confidentiality agreements regarding said Student Data. All employees with access to Student Records shall pass criminal background checks.

    b. **Destruction of Data**. Provider shall destroy all personally identifiable data obtained under the Service Agreement when it is no longer needed for the purpose for which it was obtained or transfer said data to LEA or LEA's designee, according to a schedule and procedure as the parties may reasonable agree. Nothing in the Service Agreement authorizes Provider to maintain personally identifiable data beyond the time period reasonably needed to complete the disposition.

c. **Security Protocols**. Both parties agree to maintain security protocols that meet industry best practices in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Provider shall maintain all data obtained or generated pursuant to the Service Agreement in a secure computer environment and not copy, reproduce, or transmit data obtained pursuant to the Service Agreement, except as necessary to fulfill the purpose of data requests by LEA.

d. **Employee Training**. The Provider shall provide periodic security training to those of its employees who operate or have access to the system. Further, Provider shall provide LEA with contact information of an employee who LEA may contact if there are any security concerns or questions.

e. **Security Technology**. When the service is accessed using a supported web browser, Secure Socket Layer ("SSL"), or equivalent technology protects information, using both server authentication and data encryption to help ensure that data are secure and accessible only to authorized users. Provider shall host data pursuant to the Service Agreement in an environment using a firewall that is periodically updated according to industry standards.

f. **Security Coordinator**. Provider shall provide the name and contact information of Provider's Security Coordinator for the Student Data received pursuant to the Service Agreement

g. **Subprocessors Bound**. Provider shall enter into written agreements whereby Subprocessors agree to secure and protect Student Data in a manner consistent with the terms of this Article V. Provider shall periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this Article.

2. **Data Breach**. In the event that Student Data is accessed or obtained by an unauthorized individual, Provider shall provide notification to LEA within a reasonable amount of time of the incident. Provider shall follow the following process:

   a. The security breach notification shall be written in plain language, shall be titled "Notice of Data Breach," and shall present the information described herein under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.

   b. The security breach notification described above in section 2(a) shall include, at a minimum, the following information:

      i. The name and contact information of the reporting LEA subject to this section.

      ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

      iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

c. At LEA's discretion, the security breach notification may also include any of the following:

i. Information about what the agency has done to protect individuals whose information has been breached.

ii. Advice on steps that the person whose information has been breached may take to protect himself or herself.

d. Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. Provider shall assist LEA in these efforts.

e. At the request and with the assistance of the District, Provider shall notify the affected parent, legal guardian or eligible pupil of the unauthorized access, which shall include the information listed in subsections (b) and (c), above.

ARTICLE VI: MISCELLANEOUS

1. **Term**. The Provider shall be bound by this DPA for the duration of the Service Agreement or so long as the Provider maintains any Student Data. Notwithstanding the foregoing, Provider agrees to be bound by the terms and obligations of this DPA for no less than three (3) years.

2. **Termination**. In the event that either party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated.

3. **Effect of Termination Survival**. If the Service Agreement is terminated, the Provider shall destroy all of LEA's data pursuant to Article V, section 1(b).

4. **Priority of Agreements**. This DPA shall govern the treatment of student records in order to comply with the privacy protections, including those found in FERPA and AB 1584. In the event there is conflict between the terms of the DPA and the Service Agreement, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

5. **Notice**. All notices or other communication required or permitted to be given hereunder must be

in writing and given by personal delivery, facsimile or e-mail transmission (if contact information is provided for the specific mode of delivery), or first class mail, postage prepaid, sent to the addresses set forth herein.

6. **Application of Agreement to Other Agencies**. Provider may agree by signing the Form of General Application be bound by the terms of this DPA for the services described therein for any Successor Agency who signs a Joinder to this DPA.

7. **Entire Agreement**. This DPA constitutes the entire agreement of the parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both parties. Neither failure nor delay on the part of any party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

8. **Severability**. Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

9. **Governing Law; Venue and Jurisdiction**. THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF CALIFORNIA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS LOCATED IN [Insert County] COUNTY, CALIFORNIA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS SERVICE AGREEMENT OR THE TRANSACTIONS CONTEMPLATED HEREBY.

[*Signature Page Follows*]

IN WITNESS WHEREOF, the parties have executed this California Student Data Privacy Agreement as of the last day noted below.

[District]

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

[Vendor]

By: _____ Date: _____

Printed Name: _____ Title/Position: _____

Note: Electronic signature not permitted.

EXHIBIT "A"

DESCRIPTION OF SERVICES

[INSERT DETAILED DESCRIPTION OF SERVICES HERE]

EXHIBIT "B"

SCHEDULE OF DATA

Category of Data	Elements	Check if used by your system
Application Technology Meta Data	IP Addresses of users, Use of cookies etc.	
	Other application technology meta data-Please specify:	
Application Use Statistics	Meta data on user interaction with application	
Assessment	Standardized test scores	
	Observation data	
	Other assessment data-Please specify:	
Attendance	Student school (daily) attendance data	
	Student class attendance data	
Communications	Online communications that are captured (emails, blog entries)	
Conduct	Conduct or behavioral data	
Demographics	Date of Birth	
	Place of Birth	
	Gender	
	Ethnicity or race	
	Language information (native, preferred or primary language spoken by student)	
	Other demographic information-Please specify:	
Enrollment	Student school enrollment	
	Student grade level	
	Homeroom	
	Guidance counselor	
	Specific curriculum programs	
	Year of graduation	
	Other enrollment information-Please specify:	
Parent/Guardian Contact Information	Address	
	Email	
	Phone	
Parent/Guardian ID	Parent ID number (created to link parents to students)	
Parent/Guardian Name	First and/or Last	

Category of Data	Elements	Check if used by your system
Schedule	Student scheduled courses	
	Teacher names	
Special Indicator	English language learner information	
	Low income status	
	Medical alerts	
	Student disability information	
	Specialized education services (IEP or 504)	
	Living situations (homeless/foster care)	
	Other indicator information-Please specify:	
Category of Data	**Elements**	**Check if used by your system**
Student Contact Information	Address	
	Email	
	Phone	
Student Identifiers	Local (School district) ID number	
	State ID number	
	Vendor/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	
Student In App Performance	Program/application performance (typing program-student types 60 wpm, reading program-student reads below grade level)	
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	
Student Survey Responses	Student responses to surveys or questionnaires	
Student work	Student generated content; writing, pictures etc.	
	Other student work data - Please specify:	
Transcript	Student course grades	
	Student course data	

Category of Data	Elements	Check if used by your system
	Student course grades/performance scores	
	Other transcript data -Please specify:	
Transportation	Student bus assignment	
	Student pick up and/or drop off location	

Category of Data	Elements	Check if used by your system
	Student bus card ID number	
	Other transportation data - Please specify:	
Other	Please list each additional data element used, stored or collected by your application	

EXHIBIT "C"

DEFINITIONS

AB 1584, Buchanan: The statutory designation for what is now California Education Code § 49073.1, relating to pupil records.

De-Identifiable Information (DII): De-Identification refers to the process by which the Vendor removes or obscures any Personally Identifiable Information ("PII")from student records in a way that removes or minimizes the risk of disclosure of the identity of the individual and information about them.

NIST 800-63-3: Draft National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 Digital Authentication Guideline.

Operator: For the purposes of SB 1177, SOPIPA, the term "operator" means the operator of an Internet Website, 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. For the purpose of the Service Agreement, the term "Operator" is replaced by the term "Provider." This term shall encompass the term "Third Party," as it is found in AB 1584.

Personally Identifiable Information (PII): The terms "Personally Identifiable Information" or "PII" shall include, but are not limited to, student data, metadata, and user or pupil-generated content obtained by reason of the use of Provider's software, website, service, or app, including mobile apps, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians. PII includes, without limitation, at least the following:

First and Last Name	Home Address
Telephone Number	Email Address
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
Videos	

General Categories:

Indirect Identifiers: Any information that, either alone or in aggregate, would allow a reasonable person to be able to identify a student to a reasonable certainty

Information in the Student's Educational Record

Information in the Student's Email

Provider: For purposes of the Service Agreement, the term "Provider" means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. Within the Service Agreement the term "Provider" replaces the term "Third Party as defined in California Education Code § 49073.1 (AB 1584, Buchanan), and replaces the term as "Operator" as defined in SB 1177, SOPIPA.

Pupil Generated Content: The term "pupil-generated content" means materials or content created by a pupil during and for the purpose of education including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of pupil content.

Pupil Records: Means both of the following: (1) Any information that directly relates to a pupil that is maintained by LEA and (2) 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 LEA employee.

SB 1177, SOPIPA: Once passed, the requirements of SB 1177, SOPIPA were added to Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code relating to privacy.

Service Agreement: Refers to the Contract or Purchase Order to which this DPA supplements and modifies.

School Official: For the purposes of this Agreement and pursuant to CFR 99.31 (B), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and (3) Is subject to CFR 99.33(a) governing the use and re-disclosure of personally identifiable information from student records.

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the 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 allowing online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, food purchases, political affiliations, religious information text messages, documents, student identifies, search activity, photos, voice recordings or geolocation information. Student Data shall constitute Pupil Records for the purposes of this Agreement, and for the purposes of California and Federal laws and regulations. Student Data as specified in Exhibit B is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or de-identified, or anonymous usage data regarding a student's use of Provider's services.

Subscribing LEA: An LEA that was not party to the original Services Agreement and who accepts the Provider's General Offer of Privacy Terms.

Subprocessor: For the purposes of this Agreement, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its software, and who has access to PII.. This term shall also include in it meaning the term "Service Provider," as it is found in SOPIPA.

Targeted Advertising: Targeted advertising means presenting an advertisement to a student where the selection of the advertisement is based on student information, student records or student generated content or inferred over time from the usage of the Provider's website, online service or mobile application by such student or the retention of such student's online activities or requests over time.

Third Party: The term "Third Party" as appears in California Education Code § 49073.1 (AB 1584, Buchanan) means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of pupil records. However, for the purpose of this Agreement, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT "D"

DATA SECURITY REQUIREMENTS

[INSERT ADDITIONAL DATA SECURITY REQUIREMENTS HERE]