Modern information technologies play an increasingly essential and integral role in our education system. The Software & Information Industry Association (SIIA) agrees that the effective use of student information to improve learning is concomitant with the obligation to safeguard student data privacy and security. This will require a continued trust framework between the triad of stakeholders – students/parents and schools; schools and service providers; and service providers and students/parents. As policymakers consider the need for additional federal and state regulation, this SIIA policy brief outlines a number of principles and considerations to ensure policies are appropriately targeted and crafted to ensure they do not create any unintended or unnecessary barriers to school operations and digital learning opportunities.

Education technology is increasingly vital to making certain our students receive a world class education, and our nation can compete in the global economy. Technology and data systems are mission critical in supporting K-12 educational entities and individuals – providing operational efficiencies, informing practice, and personalizing student learning. Essential to the important use of technology in education is the collection, use and sharing of student information for educational purposes. From school bus routes to student assessment results and from student lunch accounts to adaptive curriculum, our educational system has long collected, managed and applied student and other data, and has routinely done so by using the services of third-party school service providers.

School service providers view student data privacy and security as essential. They are trusted guardians of sensitive student information. Schools and service providers have a shared responsibility to protect the privacy and security of student information. One way they do this is through policies and procedures that both limit the collection and uses of student personal information to legitimate educational purposes and safeguard student privacy.

There is also a strong network of federal laws that limit the use of personally identifiable student information:

- The federal Family Educational Rights and Privacy Act (FERPA) requires that:
  - personally identifiable information shared with service providers be limited to uses otherwise performed by the school’s own employees,
  - the provider be under direct control of the school, and
  - the information can only be used for educational purposes.
FERPA and the federal Children’s Online Privacy Protection Act\(^1\) (COPPA; for children under 13) require parental consent both:
- if the school shares personal student information for non-educational purposes; and
- if the operator wants to use or disclose the information for its own commercial purposes beyond the provision of services to the school.

The federal Protection of Pupil Rights Amendment (PPRA) requires parental notice and opportunity to opt-out of activities involving the collection, disclosure, or use of personal information collected from students for marketing and advertising purposes unrelated to the educational purpose for which it was collected.

School service providers are also bound by contract, and subject to significant penalties for unauthorized disclosure. And there is a market incentive for school service providers to live up to their responsibilities. Responding to the calls for additional industry self-regulation, our organization has released industry best practices for student privacy\(^2\) as another step to ensure the safeguarding of student information. The U.S. Department of Education’s Privacy Technical Assistance Center (PTAC) also recently released further clarifying guidance.\(^3\)

These policies and agreements complete a framework of laws and practices that has been highly effective through the years in safeguarding student privacy and data security.

SIIA recognizes the importance of questions and concerns raised by some parents, educators and policymakers. SIIA agrees the obligation to safeguard student data privacy and security means that continued review and enhancements are needed in the framework of our policies, practices and technologies.

As state and federal policymakers consider policy changes, it is critical that any new regulatory requirements provide sufficient flexibility for the wide variance of circumstances – including types of technologies, types and uses of data, and local needs – so that one-size-fits-all government actions intended to create a privacy and security floor do not unintentionally create a digital learning ceiling. For example, policies should ensure that any new restrictions on the use of information for secondary purposes do not prevent teachers and parents from more effectively identifying a lesson or book appropriate to a student’s reading level in a manner long accepted in the analog world. In the compliance driven education system, policy makers must also ensure that new regulations do not create confusion or caution with a resulting chilling effect on even appropriate uses of student information.

Any new legislation should be consistent with the substantial protections in existing federal regulations to ensure new laws do not overlap, conflict, confuse and undermine those existing protections. Policymakers must ensure that new laws do not stifle the emerging use of new information technologies to improve school efficiency and implement personalized learning environments. SIIA agrees with the Obama Administration’s May 2014 report on data and privacy, which called for “Responsible Educational Innovation in the Digital Age,” including that “Students and their families need robust protection against current and emerging harms, but they also deserve access to the learning advancements enabled by technology that promise to empower all students to reach their full potential.”\(^4\)

---


The best approach is to educate, equip, and empower schools and educators to make informed decisions that safeguard student data.

Following are several areas where policymakers are considering federal and state legislation with a focus on those most specific to school service providers. For each, there is a set of factors that SIIA suggests be considered to help ensure that any new laws recognize unique circumstances and local needs.

- Definition of Student Information
- Data Governance, Transparency and Training
- Purposes for the Use and Sharing of Student Information
- Parental Consent
- Data Security
- Parental Access and Correction
- Deletion of Student Data
- Breach Notification and Penalties
- Cloud Computing
- Contract Requirements

1. Definition of Student Information

Focus on Personally Identifiable Student Information – Core to any new student privacy policies should be a limitation of their scope to personally identifiable information (PII), as is the case under existing federal law. SIIA recommends reference to PII as defined under FERPA. Use of such a standard definition is critical to ensuring consistency for families, institutions and agencies, and school service providers. Educational institutions, agencies and their service providers use de-identified, aggregate, and other anonymous information for many important educational, operational and accountability purposes that do not raise concerns about the safeguarding of student privacy and must be enabled for the delivery and improvement of educational services. New privacy policies should not regulate use of this non-identifiable information. To the extent policies do regulate non-PII, they must ensure that restrictions and requirements are adjusted according to the type of data, and therefore its sensitivity and appropriate uses.

2. Data Governance, Transparency and Training

Teachers, administrators and parents are trying to keep pace with technology innovation and the opportunity to better meet student needs through personalize learning environments. As both technologies and educational practices evolve, schools and families need support to take advantage of the opportunities, as well as to understand and address their responsibilities. One-size-fits-all mandates designed for today’s environment may unintentionally create an education and technology ceiling. A better approach is to inform and enable schools and educators to implement the tools and practices that meet student needs while safeguarding their personal data.

Public policies should first and foremost focus on the following:

- Encourage Transparency by Agencies, Institutions and Service Providers – SIIA’s best practices include: “Transparency: School service providers disclose in contracts and/or privacy policies what types of student PII are collected directly from students, and for what purposes this information is used or shared with third parties.” Transparency about service provider policies and practices empowers education officials and parents with the information they needed to make informed decisions. Encouraging transparency is an alternative to policy prohibitions that may not account for unique local or evolving circumstances.

- Ensure Appropriate Data Governance within Public Educational Agencies – Along with transparency, appropriate data governance provides a framework for education officials to

---

manage student data privacy. Governance policies put in place state and district level boards, advisory groups, etc. – composed of community members, officials, experts and other stakeholders – with responsibility for determining specific student data policies and practices. Appropriate data governance complements transparency and is an alternative to policy prohibitions that may not account for unique local or evolving circumstances.

- **Build School Technology and Human Capacity for Managing Student Data Privacy and Security** – As the education system accelerates its adoption of modern information and communication technologies, educators and educational institutions need increased federal and state support to acquire the necessary technical and human infrastructure. These supports include professional development for teachers and administrators to be good stewards of personal student information, as well as the technology tools for managing and securing that data. States and districts may consider adding chief privacy officers to provide this support. This also includes student digital literacy, as recommended by the Obama Administration’s May 2014 report on data and privacy: “Digital literacy—understanding how personal data is collected, shared, and used—should be recognized as an essential skill in K-12 education and be integrated into the standard curriculum.”

3. **Purposes for the Use and Sharing of Student Information**

SIIA agrees that information about an individual student collected or managed by a school service provider should be used only for educational purposes for which it was entrusted. The challenge is translating that principle into statute in a manner future-proofed for the wave of digital learning transformation being embraced by families and educators, at home and at school. New legislation categorically restricting “commercial” or “secondary” use of student information (including marketing or advertising) in undefined or inappropriately defined ways could block important educational innovations and learning opportunities. Any new restrictions should focus explicitly on the use of personally identifiable student information.

SIIA’s Student Privacy Best Practices include:

- “Educational Purpose: School service providers collect, use, or share student PII only for educational and related purposes for which they were engaged or directed by the educational institution, in accordance with applicable state and federal laws;” and
- “Authorization: School service providers collect, use, or share student PII only in accordance with the provisions of their privacy policies and contracts with the educational institutions they serve, or with the consent of students or parents as authorized by law, or as otherwise directed by the educational institution or required by law.”

If further policies are introduced, SIIA suggests consideration of the following:

- **School’s Need Flexibility to Operate** – In general, educational institutions and agencies must have the flexibility to determine which data to collect, with whom to share it, and for what purposes to best accomplish their operational and educational objectives. Individual parent-opt-in or opt-out are not practical for core school functions and uses. One-size-fits-all regulations may not work given the diversity of school sizes, staffing, practices and evolving uses of innovative technologies.

- **Privacy Restrictions should not Conflate “Commercial” with Appropriate Educational Uses** – Any restrictions on “commercial” uses of information should be defined so as not to unintentionally prohibit activities simply because the operator is a commercial (e.g., for-profit)

---

6 “Big Data: Seizing Opportunities, Preserving Values” Executive Office of the President, p.64 (May 2014). 
http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf
entity. Privacy restrictions should not inhibit service providers from using student information (whether PII or not) in educational uses, such as: for providing the service including through subcontractors and partners; for educational product evaluation, improvement, and development; as well as to drive recommendation engines needed to personalize learning. Among the benefits of digital learning is the ability to make ongoing improvements based on the user experience. Further, among the benefits of partnering with third-party operators is their ability to work across multiple schools and multiple applications to scale understanding of what works, and to translate that knowledge into improved services for all students and schools.

- Federal Laws Already Limit Service Providers to Educational Uses of PII – FERPA, PPRA and COPPA already provide a framework restricting collection and sharing of personal student information to educational purposes. For example, federal guidance in the area explicitly states that service providers may not use personal student information to target unrelated advertisements to students because this use “does not constitute a legitimate educational interest.”

- Encourage Use of Student Information for Educational Purposes – Rather than restricting what should not happen, public policies should encourage sound use of student information to support student learning and school operations. Public policy should enable new models that expose students, teachers, and schools to learning opportunities that “work with students like you.” Policies should allow a student or their family to receive information related to the K–12 school purposes for which student personal information was collected, and not by default prohibit that as marketing or advertising. At the least, these should be locally made determinations. Policies may also distinguish between the service provider’s “use” of the information versus their “sharing” of that information, where the latter case may appropriately be more limited. Restrictions around “marketing” or “advertising” should be limited to non-educational purposes. These unrelated uses should not be confused with use of student information to inform a teacher or family about, for example, the next module appropriate for that student or a book matching their reading level, including those provided at no additional cost to the school or student. In other words, prohibitions should not restrict the providing of information to the student or school about or related to the service they are already using.

- FERPA Authorized Uses of Information Should be Supported – Appropriate uses and disclosure of student PII under new policies should reinforce, or at least not contradict, those allowed under FERPA. These include outsourcing school functions as authorized/directed by the educational institution, research studies, audits and evaluations, public or student safety, student transfer to another school, application or matriculation to an institution of higher education, or as otherwise authorized by parental consent.

4. **Parental Consent**

Parents and guardians have a critical role in safeguarding their child’s personal information. Federal law requires parental consent if personal student information collected in schools is used or shared for non-educational purposes. FERPA allows student information to be used or shared outside the school only in certain narrowly defined circumstances, such as educational studies, service providers carrying out functions otherwise provided by a school official, and for conducting audits or evaluations. Parental consent is required for sharing or using personal student information in any other circumstances not expressly permitted by FERPA.

If further policies are introduced, SIIA suggests consideration of the following:

---

• Avoid parental Consent Requirements for Core Educational Purposes – Some have called for parental consent – either opt-in or opt-out – for all uses of personal student information, even for core educational purposes. But this is unrealistic and inefficient and for two reasons:
  - Schools need to collect information from students to operate their institutions and to provide education to their students. They must share this information with third-party providers without whom they do not have the capacity to carry out many core functions. They cannot manage their classrooms and schools if some parents exclude their children from core educational activities, thus forcing them to make endless accommodations.
  - A universal opt-in or opt-out would also unfairly create an imbalance of educational opportunity – some students would have access to the educational resources while those who opt-out, or fail to opt-in, are excluded. Requiring parents to opt-in or allowing parents to opt-out of data management would limit instructional opportunity and potentially impact student performance.

• Parental Consent Should Always be an Option Where There are Otherwise Prohibitive Restrictions – Where educational uses of student PII may go beyond that directed by the school or beyond the educational purposes related to the reason for its original collection, policies should allow for parental consent rather than strict prohibitions. This policy will empower students and families with educational opportunities that leverage and build on the information a student generates within the classroom. This is consistent with existing federal law that requires parental consent if schools and agencies want to share personal student information for purposes beyond the narrowly defined educational purposes in Federal law.

• Focus on Student Data Empowerment, Not Just Restrictions – While many legislators are focused on student data privacy protections, equal or greater attention should be focused on student data empowerment that increases student/family access to data about their children and enhances their opportunity to create a more efficient continuum between learning (digital or analog) taking place inside and outside of school. While policies should include this option in all cases, it is especially important to include given that some models provide for personal student accounts authorized by parents that extend beyond the school in purpose, use and time.

5. Data Security

SIIA agrees with the need for data security safeguards. In fact, educational institutions and agencies often turn to school service providers for their expertise in this area to provide a level of protection not often possible within a school file cabinet or data file computer servers. SIIA’s recent Student Privacy Best Practices include: “Security: School service providers have in place security policies and procedures reasonably designed to protect personal student information against risks such as unauthorized access or use, or unintended or inappropriate destruction, modification, or disclosure.” These are standard practices for the industry.

If further policies are introduced, SIIA suggests consideration of the following:

• Technical Specifications Should be Avoided – Policies should create a flexible floor that encourages innovation and competition around student data security, and does not prescribe technical measures or procedures too narrowly or in a manner that unintentionally creates a technology ceiling. Continuous evaluation and improvement of technological and procedural means is needed to ensure the security and confidentiality of student information. Vendors should be expected to implement industry-standard data privacy and security practices, but prescribing these in law and regulation could reduce incentives for related innovations and improvements.
• Data Security Should be Commensurate with Data Sensitivity – Allow for security differentiation by data types and commensurate with the sensitivity of the information, with the strongest protections for personally identifiable information that is not otherwise publicly available directory information as well as for transport and storage in public networks. Similar frameworks have already been adopted in Federal Trade Commission (FTC) regulations and the Gramm-Leach-Bliley Act, including for health and financial information.

• Shared Responsibility is Critical – Policies should recognize the shared responsibility of all stakeholders, including the roles of schools and districts where their stewardship of data hosting and access may go beyond what their service provider can otherwise secure. Student data access is largely authorized by school officials, while teachers and administrators are using and sharing that data. Service provider security technologies and protocols cannot protect against error or inappropriate use by school and agency staff. In some cases, agencies are hosting student information locally in ways that do not involve a third party service provider, putting the responsibility fully on the institutions and agencies.

6. Parental Access and Correction

Parental access and correction to educational records is a core principle of FERPA, and a functionality greatly enhanced by technology. Where appropriate and authorized, service providers already enable such access and correction as part of their service and contract. Indeed, federal law already requires schools and districts to ensure that their service providers provide appropriate access and correction. According to the recent FERPA guidance from the U.S. Department of Education: “Whenever a provider maintains a student’s education records, the school and district must be able to provide the requesting parent (or eligible student) with access to those records. Schools and districts should ensure that their agreements with providers include provisions to allow for direct or indirect parental access.”

If further policies are introduced, SIIA suggests consideration of the following:

• Requiring School Service Providers to Broker Parental Access and Corrections is Impractical and Inappropriate – In general, student educational records are not collected or managed by service providers, but are instead hosted by service providers with the management responsibility belonging to the school. In such cases, the responsibility of managing parental access and correction controls should also be with the school and not the service provider. It is the school that has the relationship with the parent manages and controls access and correction. In cases where there is a personal student account or where the model is designed for direct parental interaction, it may be more appropriate for service providers to broker parental access.

• Limit Access and Correction to Educational Records – Public policies should not extend access and correction obligations to all types of data collected through student use of third-party services and applications. This would raise questions of scope, appropriateness and workability. Not all of this information is personally identifiable, and much of it is not part of the student’s educational record. For example, data types could include keystroke transactional data, responses to group classroom-level formative assessments, or answers to questions embedded in a software program intended only for adaptive diagnostic purposes. While parental (and student) access should be encouraged and enabled wherever possible, it is unclear that access and correction can or should be extended in all cases that go beyond the traditional notion of personally identifiable information from a student’s educational record.

---

• **Ensure Flexibility for Access and Correction Mechanisms** – Where a school wants to, or is obligated to, provide access and correction to student information, public policies should not dictate the implementing process or technology. It is common practice for service providers to satisfy a school access requirement, for example, by exporting student data back into a single parent accessible portal per the school’s preference. New legislation should not mandate, for instance, direct parental access, because if a product is not designed to provide this access, there would be a significant product and process modification needed to make it so and other means may be more appropriate.

• **Move Toward Direct Student/Family Control of Student Data** – Over time, there is opportunity to extend the direct relationship between families (and students, especially over 18) and service providers serving their children at school, thus further empowering students and parents with more direct access and control of their information for additional uses. The U.S. Department of Education’s MyData initiative is a step in this direction, encouraging schools to enable students to access and download that student’s own academic data in a machine-readable format to create a personal learning profile that the student can keep throughout their learning career. Data uses might include requests for recommendations on instructional modules targeted to a student’s unique needs beyond what is being provided through the school. Uses also include portable portfolios that a student uses throughout their academic and professional career, similar to emerging models for individual health records. Finally, it is important to recognize that family control of student data for additional purposes should not be confused with a parent opt-in or opt-out of a school’s sharing of PII with service providers for purposes otherwise performed by the school’s own employees.

7. **Deletion of Student Data**

In general, the deletion of personally identifiable student data no longer needed for the purpose for which it was collected is a sound principle, and one that should be core to school policies and service provider practices. However, one-size-fits-all requirements are impractical due to the variance in data types and uses, as well as in governance. To override school or student preferences with a mandatory deletion requirement is not flexible enough to cover all the situations in which data might need to be retained.

If further policies are introduced, SIIA suggests consideration of the following:

• **Recognize that Deletion is Often Under Direct Control of Schools** – Personal student information is often under the direct control of the school and not the service provider, such that service providers often do not have access or authorization to delete that information. In most other cases, service provider use – including deletion – of personally identifiable student information is determined and directed by school requirements.

• **Differentiate Deletion Policies by Types and Uses of Student Data** – Deletion policies must differentiate between types and uses of student information. Privacy deletion requirements should only address personally identifiable information, which is of primary interest with regard to a student’s privacy. Absolute data deletion requirements for aggregated, de-identified and other anonymous data that do not pose a concern for a student’s privacy will jeopardize the important and necessary use of this information for ongoing educational purposes. These include the use of non-identifiable information as the fuel for adaptive software, learning analytics and other algorithmic engines whose benefit is that they get ‘smarter’ based on a continuing flow of usage data. Personal student information may also be needed on an ongoing basis such as for district

---

and state longitudinal accountability systems as well as future transcript and degree verification requests from employers and postsecondary institutions.

- **Deletion Requirements are Not Appropriate for Personal Accounts** – Increasingly, data governance is shared between the school and the student or student’s parents such as when a student uses a personal account, perhaps created initially for school purposes, to access educational applications and related information. In this model, the intent may be for student information to travel with the student outside and beyond their school, such as documents they created or information about their performance on a mathematics tutorial software application. As such, deletion decisions fall largely with students and parents, and a mandatory deletion requirement would deny them future access to their own information.

- **De-identification is an Alternative to Deletion** – De-identification is a well-accepted legal and industry practice that serves as an appropriate alternative to deletion. De-identification is especially important to ensure that aggregate and meta-data can be maintained to support algorithmic engines and accountability systems. Public policy should accommodate this need to retain de-identified data.

8. **Breach Notification and Penalties**

SIIA recognizes the concern for the potential unauthorized access to a student’s sensitive personal information and the inclination for policymakers to respond with harsh data breach penalties as a deterrent. SIIA concerns include the potential duplication and conflict with existing federal and state data breach notification laws, lack of clarity regarding the criteria for penalties, and the chilling effect on the sector from criminal penalties.

If further policies are introduced, SIIA suggests consideration of the following:

- **Rely on Existing Breach Laws and Avoid Regulatory Conflicts** – There is already a strong regulatory framework in place regarding corporate breach of contract and privacy policies, data breach notification requirements, and related penalties. Policymakers should rely on existing general laws that also apply to the education sector, and only advance additional policies if there are gaps. New policies should also ensure there is not overlap or conflict, including with investigative jurisdiction, criteria for violation, and penalties.

- **Include Clear Criteria for What Constitutes a Breach of Law** – Laws that provide penalties for violations must be clear in what constitutes a violation, and the criteria for that violation. In cases where the legal requirement is broad, service providers may be unclear what constitutes compliance. In cases where the obligation is to address a local district policy, laws must ensure that districts make their service providers aware of any unique local requirements. In the case of penalties, states should carry out a rulemaking to define the criteria for violations and the process for determining violations and penalties. Where the breach is not intentional or malicious, do not treat disclosure of each student’s data as a separate violation with regard to penalties.

- **Follow Standards for Breach Threshold** – Ensure breach notification requirements and penalties follow industry and legal threshold standards. Even in the financial and health sectors, breach notification requirements include exceptions in cases such as for non-identifiable or non-sensitive information, where there is no harm, and where the disclosure was internal and unintentional such as to another provider or school employee.

- **Avoid Criminal Penalties** – Legal standards for penalties require knowledge of a violation, and either gross negligence or criminal intent. In cases such as unauthorized distribution and inadvertent release of student data, penalties should be financial and related to an entity’s ability
to continue doing business. Criminal penalties should be avoided as no states have criminal and prison penalties for data breaches or violations of breach notification requirements, and the threat of imprisonment will be a disincentive for service providers to operate in schools and states.

9. Other

- **Cloud Computing.** Regulations Should Not Restrict Data Location or Cloud Computing – New technologies provide enhanced access and security at reduced cost through remote data hosting – often called “cloud computing.” Public policies that prohibit student data from leaving the state will reduce school and agency flexibility to access these tools, thus limiting functionality and adding costs. Similarly, policies must recognize that hosted data models increase security and reduce costs by randomizing the location of that data, thus making impractical transparency policies that too narrowly require exact data location identification.

- **Contract Requirements.** Contract Requirements Must Allow for Flexibility Between Agencies and Service Providers – Policies that dictate contract terms must be careful to not impose one-size-fits-all requirements where circumstances and needs may vary. Any state requirements for school agency contracts should be outlined broadly and should provide a template identifying what issues should be addressed rather than prescribing the specific terms.

- **Biometric Data.** Do not Categorically Prohibit the Collection and Use of Biometric Data – Biometric data and related student information is increasingly used for a variety of important educational purposes, including for student identification and student learning. Full prohibitions will disrupt school operations and inhibit learning opportunities. For example, retina and fingerprint identification is used for identification and security related to online testing and virtual learning, as well as for device security that helps secure student data. Use of biometric data for instructional purposes includes voice to text for deaf or other students, voice recording and diagnostics for reading or foreign language learning, and eye tracking for diagnostics in reading comprehension. In many cases, this data need not be identifiable or collected, thus reducing privacy concerns. Where it is necessary for the biometric data to be collected and/or personally identifiable, alternative approaches can include restrictions on inclusion in a student’s permanent educational record, requirements for deletion, and other security measures such as encryption to protect unauthorized access.

SIIA agrees with the need to safeguard student data privacy and security. As the considerations above suggest, legislation built around one-size-fits-all requirements and prohibitions have the danger of falling far short in a dynamic environment of educational change and technology innovation. This caveat does not mean that further protections may not be appropriate, but simply that they need to be very carefully crafted. Policymakers need to be careful that privacy protection floors do not inadvertently and unnecessarily lead to educational ceilings that inhibit operations and limit innovation and opportunity. SIIA instead encourages new policies to be focused on transparency and governance to empower parents and school officials with the information about data collection, use and disclosure needed to make sound and safe use of student information that focus on the goal of advancing student learning.

---

The Software & Information Industry Association (SIIA) is the principal trade association for the software and digital content industry. SIIA provides global services in government relations, business development, corporate education and intellectual property protection to more than 800 leading software and information companies. The SIIA Education Division serves and represents more than 200 member companies that develop software, digital content and other technologies that serve educational needs. The Division shapes and supports the industry by providing leadership, advocacy, business development opportunities and critical market information. For more information, visit [www.siiainc.com](http://www.siiainc.com).