

November 1, 2017

As you may recall, [HB 16-1423](#) (C.R.S. 22-16-101, *et seq.*) made a number of significant changes to Colorado law pertaining to Student Data Transparency and Security. These requirements apply to all Local Education Providers, including school districts, charter schools, and BOCES; however, the purpose of this guidance is to provide additional information to CSI charter schools and so the term “school” will be used throughout.

The following is provided for informational purposes only and is not to be construed as legal advice or a formal legal opinion on behalf of the author or CSI. Use of this information does not create an attorney-client relationship, nor is the creation of such relationship intended by the provision of this information. This information does not constitute a formal administrative opinion on behalf of CSI. CSI recommends that each school contacts its attorney to obtain legal advice with respect to any particular legal issue.

## BACKGROUND INFORMATION

Known as the Student Data Transparency and Security Act (“the Act”), the Act sets forth specific requirements for contracts entered into with School Service Contract Providers (“Contract Providers”) and On-Demand Providers (see C.R.S. 22-16-101, *et seq.*). Depending on the type of vendor (Contract Provider versus On-Demand Provider), different requirements apply. Accordingly, it is imperative to first understand whether a vendor is a School Service Contract Provider or an On-Demand provider.

**School Service Contract Provider:** An entity, other than a Public Education Entity<sup>1</sup> or an Institution of Higher Education, that enters into a formal, negotiated contract with a Public Education Entity to provide a School Service. A “School Service” is a website, online service, or app that is (i) designed and marketed primarily for use in a pre-k, elementary, or secondary school; (ii) used at the direction of teachers or other employees of the school; and, (iii) which collects, maintains, or uses Student Personally Identifiable Information (“Student PII”).<sup>2</sup>

➤ *E.g., Google Apps for Education, Infinite Campus or PowerSchool, or Edgenuity*

**On-Demand Provider:** School Service On-Demand providers (“On-Demand provider”) are entities, other than a Public Education Entity, that provide a school service on occasion to a school, subject to agreement by the school or one of its employees to standard, non-negotiable terms and conditions of services established by the On-Demand provider. Unlike Contract Providers, On-Demand providers do not require a formal, negotiated contract; rather, an On-Demand provider would be something like an app that provides a school service that can be downloaded by a teacher that asks a teacher to click to agree with the vendor’s Terms of Service.

<sup>1</sup> “Public Education Entity” means CDE, a local education provider, CSI, or a public school. A “Local Education Provider” is a school district, charter school (district or CSI), or a BOCES.

<sup>2</sup> This definition does not include an internet website, online service, online application, or mobile application that is designed and marketed for use by individuals or entities generally, even if it is also marketed to a United States preschool, elementary school, or secondary school.

CDE has issued [guidance on how to tell whether a provider is a Contract Provider or an On-Demand provider](#). With both instances, you must first determine whether the provider provides a “school service.”<sup>3</sup>

## I. CONTRACTS ENTERED INTO OR RENEWED WITH SCHOOL SERVICE CONTRACT PROVIDERS AFTER AUGUST 10, 2016

[CSI issued guidance in June of 2016](#) regarding the immediate implications of HB 16-1423; namely, the requirement that all contracts entered into or renewed on or after August 10, 2016 with School Service Contract Providers contain certain contract provisions pertaining to the use of Student PII. In summary, **all contracts entered into or renewed with a School Service Contract Provider must include terms requiring the Contract Provider to comply with the following:**

### 1. Data Transparency Requirements

- a. The Contract Provider must provide clear information to the school explaining (i) the data elements of Student PII that it collects, whether it is collected upfront or ultimately held in the aggregate; (ii) the learning purpose for which it collects the data; and (iii) how it uses and shares the Student PII. This information should be easily accessible through a website, and the school must post the information on its website (more information on posting requirements is provided below).
- b. The Contract Provider must provide notice to the school prior to making any material changes to its privacy policy for school services.
- c. The Contract Provider must provide access to and correction of any factually inaccurate Student PII that is requested by the school.
- d. If the Contract Provider discovers misuse or unauthorized release of Student PII by the Contract Provider, one of its subcontracts, or a subsequent subcontract, the Contract Provider must notify the school as soon as possible, regardless of whether the breach is material.

### 2. Use of Data

- a. The Contract Provider can collect, use, and share Student PII only for the purposes authorized in the contract, or with the consent of the student<sup>4</sup> or parent.
- b. The Contract Provider must obtain the consent of the student or parent before using Student PII in a manner that is inconsistent with the Contract Provider’s privacy policy or the contract with the school.
- c. The Contract Provider cannot:
  - i. Sell Student PII<sup>5</sup>;
  - ii. Use or share Student PII for purposes of targeting advertising to students;
  - iii. Use Student PII to create a personal profile of a student other than for supporting purposes authorized by the school or with the consent of the student or parent.

---

<sup>3</sup> E.g., a website, online service, or app that is (i) designed and marketed primarily for use in a pre-k, elementary, or secondary school; (ii) used at the direction of teachers or other employees of the school; and, (iii) which collects, maintains, or uses Student Personally Identifiable Information (“Student PII”).

<sup>4</sup> Student consent to the use, sharing, or retention of Student PII is only valid if the student is at least 18 years old or legally emancipated.

<sup>5</sup> This prohibition does not apply to the purchase, merger, or other acquisition of the Contract Provider provided the successor entity continues to be subject to the terms of the contract and the Colorado student data privacy laws.

- d. The Contract Provider can use or disclose Student PII consistent with HB 16-1423<sup>6</sup> but must notify the school as soon as possible after the use or disclosure.
- e. The Contract Provider can use or disclose Student PII to a subcontractor only if it contractually requires the subcontract to comply with the same requirements of HB 16-1423.

3. Data Security and Destruction

- a. The Contract Provider must maintain a comprehensive information security program designed to protect the Student PII.
- b. If a school requests destruction of a Student's PII during the term of the contract, the Contract Provider must destroy the information as soon as practicable after the date of the request unless it obtains the consent of the student or parent or the student has transferred to another school and the other school requests that the information be retained.
- c. Following the termination or conclusion of the contract, the Contract Provider, within the time period specific in the contract, must destroy all Student PII collected, generated, or inferred as a result of the contract. If the contract does not specify a time period for destruction, the Contract Provider must destroy the information when it is no longer needed for the purpose of the contract. The Contract Provider must notify the school of the date that it destroys the Student PII.

CDE has created [sample contract templates](#) that can be referenced in creating these contracts.

## II. PARENT COMPLAINT POLICY

Pursuant to the Act, parents have certain rights regarding the school's use of Student PII. These rights include:

- a. The right to inspect and review the Student PII that is maintained by the school for their student;
- b. The right to request a paper or electronic copy<sup>7</sup> of their child's Student PII, including that which is maintained by a Contract Provider; and
- c. To request corrections to factually inaccurate Student PII maintained by the school. After receiving such request, the school must correct the factual inaccuracy and confirm the correction to the parent within a reasonable amount of time.

**Each school's governing board must adopt a policy for hearing complaints from parents regarding the school's compliance with C.R.S. 22-16-101, et seq..** At a minimum, the policy must provide the parent the opportunity to submit information to the governing board and receive a hearing by the board, and the board must take action on the parent's complaint within 60 days

---

<sup>6</sup> E.g., to ensure legal or regulatory compliance; respond to or participate in the judicial process; protect the safety of users; or investigate a matter of public safety.

<sup>7</sup> If an electronic copy is requested, the school must provide the electronic copy unless it does not maintain Student PII electronically and reproducing it in an electronic format would be unduly burdensome.

after the hearing. This can be in the school's Student Information Privacy and Protection Policy, can be added to your Grievance Policy, or can be a stand-alone policy.

### III. ONLINE POSTING REQUIREMENTS

The Act includes various requirements for online posting of information relating to student data privacy and security. Each school must post and maintain the following on its website:

- Clear information explaining the data elements of Student PII that the school collects and maintains in its data system (not including the Student PII that it transmits to CDE). The list must explain how the school uses and shares the Student PII.
- A link to the index of data elements that the state board publishes. The link is: <http://www.eddataportal.info/cde>
- A list of the Contract Providers with which it contracts and a copy of each contract.
- As mentioned under Section (1)(1)(a) above, the information from the Contract Provider regarding the data elements of Student PII it collects, the learning purpose for which it collects it, and how the Contract Provider uses and shares the information. The Contract Provider must provide this in a format that is easily accessible through a website, and the school must post this information.
- The school's current Student Information Privacy Protection Policy.
- If using any On-Demand service providers:
  - To the extent practicable, a list of the On-Demand providers that the school or one of its employees uses for school services. At a minimum, this list must be updated at the beginning and mid-points of each school year.
  - A list of any On-Demand providers that it ceases using or refuses to use because the On-Demand provider (i) fails to comply with its own privacy policy; (ii) sells Student PII for an impermissible purpose, uses or shares Student PII for purposes of targeted advertising to students, or uses Student PII to create a personal profile of a student for purposes outside the contract or without the consent of the student or student's parents; or, (iii) fails to maintain a comprehensive security program to protect Student PII. The school must also post any written response from the On-Demand provider after it has been notified it will no longer be used.
  - A notice to On-Demand providers that, if the school ceases using or refuses to use an On-Demand school service provided for the reasons set forth above, the school will post on its website the name of the On-Demand provider, with any written response received, and will notify the CDE, which will also post on its website the On-Demand provider's name and any written response (this information, along with information about how to send this information to CDE, will be posted on CDE's [On-Demand Provider Transparency](#) page).

**For an example of these online posting requirements, please visit the [St. Vrain Valley Schools Student Data Transparency and Security Act](#) webpage.** Please note that as of the date of this guidance, St. Vrain Valley does not yet have their Student Information Privacy Protection Policy posted.

### IV. STUDENT INFORMATION PRIVACY AND PROTECTION POLICY

Each school must adopt a Student Information Privacy and Protection Policy by December 31, 2017.<sup>8</sup> The policy must address the following elements, at a minimum:

- a. Creating and maintaining a student data index;
- b. Retention and destruction of Student PII;
- c. Using Student PII for purposes internal to the school;
- d. Preventing breaches in the security of Student PII (not just as it relates to third-party vendors);
- e. Responding to any security breaches that occur;
  - i. The policy should include a process for addressing security breaches overall and not just vendor breaches.
  - ii. Regarding School Service Contract Providers specifically, the policy must require the board, within a reasonable time after the school identifies the existence of a material breach, to hold a public hearing that includes discussion of the nature of the material breach, an opportunity for the Contract Provider to respond, public testimony, and a decision as to whether to direct the school to terminate or continue the contract.
  - iii. Regarding breaches by On-Demand Providers specifically, the policy must include procedures addressing the instance in which the school receives evidence that an On-Demand provider does not (i) comply with its own privacy policy; (ii) sells Student PII for an impermissible purpose, uses or shares Student PII for purposes of targeted advertising to students, or uses Student PII to create a personal profile of a student for purposes outside the contract or without the consent of the student or student's parents; or, (iii) fails to maintain a comprehensive security program to protect Student PII. These procedures should address:
    - A. Whether to cease using the On-Demand provider;
    - B. Notifying the On-Demand provider that it is ceasing or refusing to use the On-Demand provider;
    - C. Providing the On-Demand provider an opportunity to respond in writing; and
    - D. Posting this information on the school's website, and notifying CDE of the same.
- f. Contracting with Contract Providers and using school services provided by On-Demand providers;
  - i. The policy must include a statement that the school will not enter into or renew a contract with a Contract Provider that refuses to abide by the requisite contract terms and requirements set forth by the Act.
  - ii. The policy should also address the requirements for posting the requisite information on the school's website.
- g. Disclosing Student PII to Contract Providers, On-Demand providers, or other third parties;
- h. Notifying parents regarding collection of, retention of, and access to Student PII;
- i. Notifying parents of their rights relating to the Student PII maintained by the school, and the complaint policy discussed above (Section II)<sup>9</sup>;
- j. Providing training in student information security and privacy to employees of the school;

---

<sup>8</sup> HB 16-1423 extends this deadline to July 1, 2018 for small rural districts, but does not clarify whether the deadline can be extended for charter schools.

<sup>9</sup> This can be a separate policy, or included in the Student Data Security Policy.

- k. Requiring the school's board to annually review the Student Information Privacy and Protection Policy and make any revisions as necessary to stay current and adequately protect Student PII in light of advances in data technology and dissemination;
- l. Addressing that the school will make copies of this policy upon request to the parent of an enrolled student and shall post a current copy of the policy on the school's website.

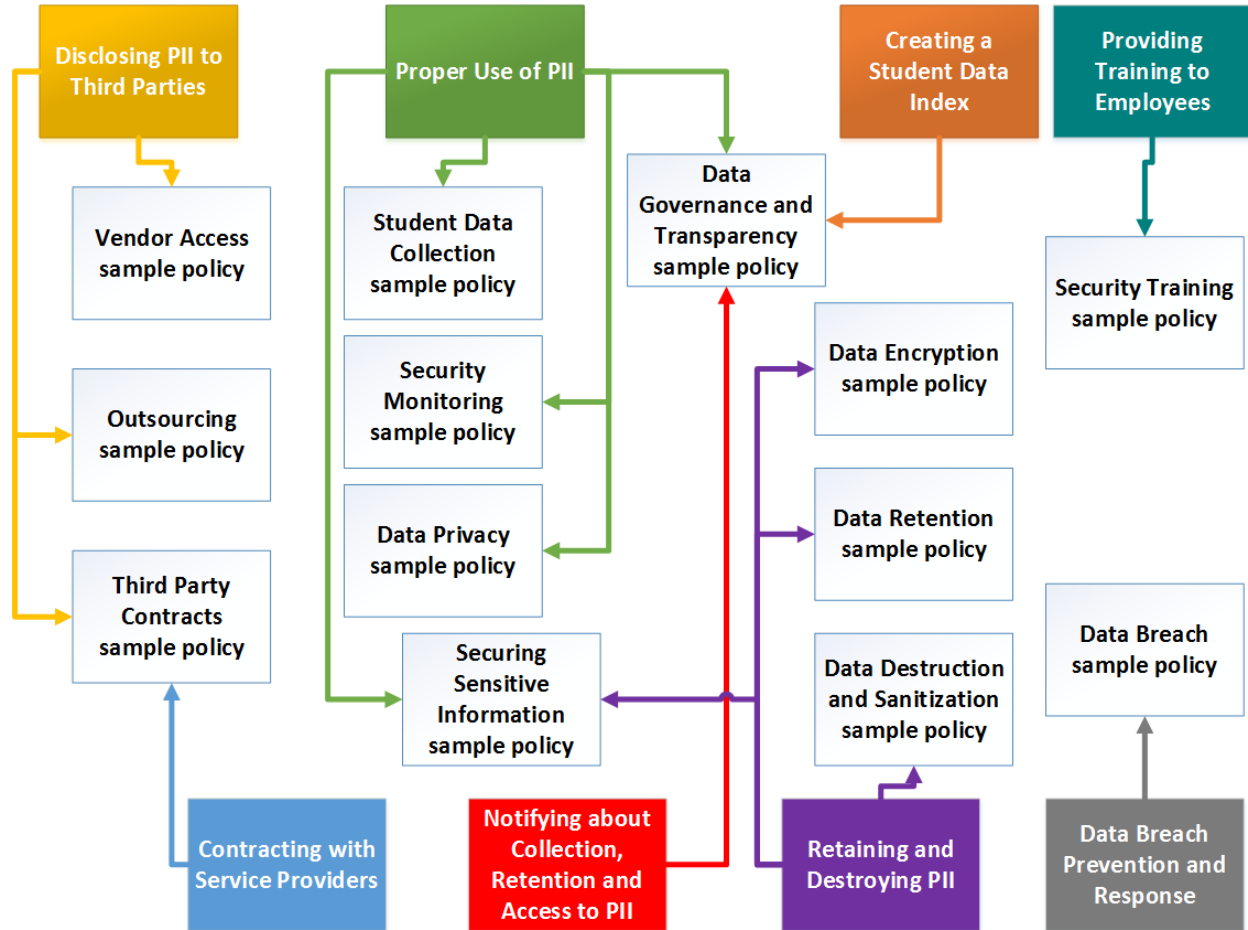
CDE has created a [suite of sample policies](#) that address the elements above. Attached to this guidance is a crosswalk of policy requirement to sample CDE policy, as well as a compliance checklist for policy and online posting requirements. CDE's policies are completely optional and may include provisions that extend beyond the minimum requirements set forth by the Act. Schools can adopt any or all of the sample policies, compile the policies into one larger student data privacy policy, or create their own policies so long as the school is addressing the elements set forth above.

### **CONCLUSION**

CSI will be auditing schools' compliance with the above requirements in January of 2018 and will provide feedback to each school. A reminder will be sent out in advance of the audit. For additional resources and information, please visit the CDE's [New Data Privacy Law Resources](#) webpage.

For questions or comments, please contact Trish Krajniak, CSI Director of Legal and Policy Initiatives ([trishkrajniak@csi.state.co.us](mailto:trishkrajniak@csi.state.co.us); 303.866.6960).

### CDE POLICY CROSSWALK



Student Data Privacy and Protection <u>Policy Compliance</u> Checklist		
Requirement	Check	Sample CDE Policy <i>*Note: CDE's sample policies are optional and contain provisions that extend beyond the minimum statutory requirements. CSI Schools are encouraged to review the sample policies and tailor them to meet the needs of the school, provided that minimum requirements are being met. .</i>
<b>The policy addresses creating and maintaining a student data index</b> [e.g., addresses the requirement that the school post and maintain on its website a clear explanation of the Student PII the school collects (not including the info transmitted to CDE); addresses the requirement that the school post on its website a link to the data inventory/data index published by the state board].		Data Governance and Transparency
<b>The policy addresses retention and destruction of Student PII</b> [e.g., addresses what information is encrypted; how Student PII is stored; how long Student PII is retained; destroying and sanitizing Student PII].		Data Encryption  Data Retention  Data Destruction and Sanitization
<b>The policy addresses using Student PII for purposes internal to the school</b> [e.g., security in collecting and storing information; monitoring security of Student PII; what information can/cannot be shared or accessed by others, etc.].		Data Governance and Transparency  Student Data Collection  Security Monitoring  Data Privacy  Securing Sensitive Information
<b>The policy addresses preventing breaches</b> [e.g., all breaches of Student PII and not just vendor breaches].		Data Breach
<b>The policy addresses responding to any security breaches</b> [e.g., any breaches of Student PII, not just breaches by vendors; includes specific provisions for breaches by School Service Contract Providers (public hearing by board w/in reasonable time after identifying existing of breach that includes discussion re: nature of the breach + opportunity for Contract Provider to respond + opportunity for public testimony + decision as to whether to terminate contract); specific provisions regarding breaches by On-Demand Provider (procedures for addressing breach must include discussion of whether to cease using On-Demand Provider + notifying the On-Demand		Data Breach  <u>CDE Webpage on On-Demand Providers</u>



Provider if ceasing to use + providing On-Demand Provider opportunity to respond in writing + posting this info on school's website + notifying CDE].		
<b>The policy addresses requirements for contracting with Contract Providers and using services by On-Demand Providers</b> [e.g., statement that the school will not enter into or renew a contract with a Contract Provider that refuses to abide by the requisite contract terms regarding Data Transparency, Use of Data, and Data Security and Destruction, or provisions relating to material breach; addresses the requirements for posting requisite information school's website].		Third Party Contracts  See Section I of CSI's Guidance Document for contract provision requirements  See Section III of CSI's Guidance Document for online posting requirements
<b>The policy addresses disclosing Student PII to Contract Providers, On-Demand Providers, or other third parties</b> [e.g., information that a vendor can/cannot access; vendor responsibilities and internal controls; what can/cannot be outsourced to a third-party vendor; contract requirements].		Vendor Access  Outsourcing  Third Party Contracts
<b>The policy addresses notifying parents regarding collection of, retention of, and access to Student PII</b> [e.g., the information that is collected, who can access, etc.].		Data Governance and Transparency
<b>The policy addresses notifying parents of their rights relating to the Student PII maintained by the school and the complaint process</b> [e.g., right to inspect/review Student PII maintained by school, request paper or electronic copy of Student PII, right to request corrections of Student PII; also includes a board-adopted complaint process regarding school's compliance with the Act that provides parents the opportunity to submit information to the school's board + board must take action on complaint w/in 60 days after hearing]. Note: The complaint process can be included in the Student Data Privacy Policy, be a stand-alone policy, or be included in the school's grievance policy.		See Section II of CSI's Guidance for complaint policy requirements
<b>The policy addresses providing training in student information security and privacy to employees of the school</b> [e.g., the training that is provided; who is responsible for providing training; who must attend training; topics covered, etc.].		Security Training
<b>The policy requires the school's board to annually review the policy and make any revisions as necessary to stay current and adequately protect Student PII in light of advances in data technology and dissemination.</b>		N/A
<b>The policy addresses that the school will make copies of this policy upon request to the parent of an enrolled student and shall post a current copy of the policy on the school's website.</b>		N/A

## Student Data Privacy and Protection Online Posting Checklist

Requirement	Check	Resource
<b>Clear information explaining the data elements of Student PII that the school collects and maintains in its data system (not including the Student PII that it transmits to CDE). The list must explain how the school uses and shares the Student PII.</b>		Data Governance and Transparency
<b>A link to the index of data elements that the state board publishes. The link is: <a href="http://www.eddataportal.info/cde">http://www.eddataportal.info/cde</a></b>		<a href="http://www.eddataportal.info/cde">http://www.eddataportal.info/cde</a>
<b>A list of the Contract Providers with which it contracts and a copy of each contract.</b>		N/A
<b>The information from the Contract Provider regarding the data elements of Student PII it collects, the learning purpose for which it collects it, and how the Contract Provider uses and shares the information.</b> The Contract Provider must provide this in a format that is easily accessible through a website, and the school must post this information.		This is provided by the Contract Provider. See Section (l)(1)(a) of CSI's Guidance Document
<b>The school's current Student Information Privacy Protection Policy.</b>		N/A
<b>If using any On-Demand Providers:</b>		
<b>A notice to On-Demand Providers</b> that, if the school ceases using or refuses to use an on-demand school service provided for the reasons set forth above, the school will post on its website the name of the On-Demand Provider, with any written response received, and will notify the CDE, which will also post on its website the On-Demand Provider's name and any written response (this information, along with information about how to send this information to CDE, will be posted on CDE's On-Demand Provider Transparency page).		Can use language from the statute  <u><a href="#">CDE Webpage on On-Demand Providers</a></u>
<b>A list of any school service On-Demand Providers that it ceases using or refuses to use</b> because the On-Demand Provider's (i) fails to comply with its own privacy policy; (ii) sells Student PII for an impermissible purpose, uses or shares Student PII for purposes of targeted advertising to students, or uses Student PII to create a personal profile of a student for purposes outside the contract or without the consent of the student or student's parents; or, (iii) fails		N/A

<p>to maintain a comprehensive security program to protect Student PII. <b>The school must also post any written response from the On-Demand Provider after it has been notified it will no longer be used.</b></p>		
<p><b>To the extent practicable, a list of the school service On-Demand Providers that the school or one of its employees uses for school services.</b> At a minimum, this list must be updated at the beginning and mid-points of each school year.</p>		<p>N/A</p>