Local education provider (LEP) must adopt a policy:
- Providing for a public hearing on the LEP’s Board of Education (BOE) determining whether to terminate the contract with SSCP because SSCP committed a material breach. (C.R.S. § 22-16-107(2)(a))
- Must have discussion of nature of material breach, opportunity for school service contract providers (SSCPs) to respond, public testimony, and a decision as to whether to direct LEP to terminate or continue the contract
- Providing a hearing procedure for parent/guardian (P/G) complaints regarding LEP’s compliance with the Act. (C.R.S. § 22-16-102(1)(a))
- P/G must have opportunity to submit information to the BOE, receive a hearing by the BOE, require BOE to take action on P/G’s complaint within 60 days after the hearing
- Providing for student information privacy and protection that addresses: (C.R.S. § 22-16-107(4)(a)); referencing C.R.S. § 22-16-108(1))
- Authorizing access to student personally identifiable information (SPII), including how access is authenticated);
- Privacy and security audits;
- Security breach planning, notice and procedures; data retention and destruction procedures; data collection and sharing procedures; provisions that safeguard privacy and security and includes penalties for noncompliance with respect to contracts involving databases, assessments or instructional supports including SPII
- Security practices for privacy when using online education services, including websites and applications
- Contracts involving outsourcing of educational services
- Contracts involving online education services
- Publishing a list of vendors that LEP contracts with that hold SPII
- Consequences for security breach
- Staff training regarding policy compliance
- Must annually review and update these policies, make copies of the policy upon request to parents/guardians of students enrolled in LEP, and post current policy on its website. (C.R.S. § 22-16-107(4)(c))

Local education provider (LEP) must post and maintain on its website:
- Clear information, understandable to a layperson, explaining the data elements of student personally identifiable information (SPII) that it collects and maintains in its data system (not including SPII sent to CDE). (C.R.S. § 22-16-107(1)(a))
- Must explain how LEP uses and shares SPII
- Link to data inventory and disclosure or CDE’s index of data elements. (C.R.S. § 22-16-107(1)(b))
- List of school service contract providers (SSCPs) that LEP contracts with and a copy of each contract. (C.R.S. § 22-16-107(1)(c))
- Information received from SSCP(s) with which LEP contracts including: (i) data elements of SPII that SSCP collects; (ii) learning purpose for which SSCP collects SPII; (iii) how SSCP uses and shares SPII. (C.R.S. § 22-16-108(1))
- To extend practicable, a list of school service contract providers (SSCPs) that any LEP employee uses for school services (SS)). (C.R.S. § 22-16-108(1))
- LEP must assist parent/guardian (P/G) to obtain data privacy policy of SSCP(s). (C.R.S. § 22-16-107(2)(a))
- If P/G has evidence demonstrating that a SSCP does any of the following, then P/G may notify LEP and provide evidence: (i) SSCP does not substantially comply with its privacy policy; (ii) SSCP uses SPII; (iii) SSCP uses SPII for targeted advertising to students; (iv) SSCP uses SPII to create a personal profile of a student other than for supporting purposes authorized by LEP and with consent of student or student’s P/G; or (v) SSCP does not maintain the comprehensive information security program reasonably designed to protect security, privacy, confidentiality, and integrity of SPII with appropriate administrative, technological and physical safeguards. (C.R.S. § 22-16-107(2))
- Destroy all SPII collected, generated or inferred as part of the contract with the LEP within the time period specified in contract with LEP or if LEP requests destruction during term of contract, then as soon as practicable after the date of request unless: (i) SPII is obtained consent of S or S’s P/G to retain SPII or (ii) S has transferred to another public school and receiving school has requested the SSCP retain the related SPII. (C.R.S. § 22-16-110(2))
- LEP may not enter into or renew contract with SSCP that SPII refuses to accept these terms or has substantially failed to comply with these terms. (C.R.S. § 22-16-107(2)(a))
- LEP must determine whether to terminate a contract with an SSCP that commits a material breach of the contract involving the misuse or unauthorized release of SPII in accordance with District policy. (C.R.S. § 22-16-107(2)(a))
- SPII may be allowed to: (C.R.S. § 22-16-108(3))
  - Use or disclose SPII to: (i) ensure legal or regulatory compliance or take precautions against liability; (ii) respond to or participate in judicial process; (iii) protect the safety of users or others on SSCP’s website, online service, online application or mobile application; and (iv) investigate a matter of public safety.
  - Disclose SPII to subcontractor only if subcontractor is required to comply with same terms of items listed above.
# FRAMEWORK FOR UNDERSTANDING THE STUDENT DATA TRANSPARENCY AND SECURITY ACT

## DEFINITIONS

<table>
<thead>
<tr>
<th>Aggregate data</th>
<th>FERPA</th>
<th>OTHER CONSIDERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>De-identified data (anonymized data)</strong></td>
<td>Data collected and reported at the group, cohort, or institutional level that is aggregated using protocols that are effective for preserving the anonymity of each individual included in the data. (C.R.S. § 22-16-103(1))</td>
<td>Release of education records that have been de-identified is not considered a &quot;disclosure&quot; under FERPA because de-identified data does not contain personally identifiable information that can lead to identification of individual students. De-identified data may be shared without the consent required by §99.30 with any party for any purpose, including parents, general public, and researchers after removing all PI that provided that the educational agency or institution or other party has made reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases and taking into account other reasonably available information. (34 CFR § 99.31(b)(1))</td>
</tr>
<tr>
<td><strong>Destroy</strong></td>
<td>To remove student personally identifiable information so that it is permanently irretrievable in the normal course of business. (C.R.S. § 22-16-103(3); C.R.S. § 22-16-110(3))</td>
<td>An educational agency or institution must not destroy any education records if there is an outstanding request to inspect and review records. (34 CFR § 99.10(3))</td>
</tr>
<tr>
<td><strong>Student (eligible student)</strong></td>
<td>A student at least 18 years of age or legally emancipated may consent to the use, sharing or retention of the student's student personally identifiable information (SPII). (C.R.S. § 22-16-109(4))</td>
<td>A student is an individual who has been in attendance at an educational agency or institution and regarding whom the agency or institution maintains education records. An eligible student is one who has reached 18 years of age or is attending a postsecondary institution at any age. (34 CFR § 99.33)</td>
</tr>
<tr>
<td><strong>School service</strong></td>
<td>An internet website, online service, online application, or mobile application that: • is designed and marketed primarily for use in a preschool, elementary school, or secondary school; • is used at the direction of teachers or other employees of a local education provider; and • Collects, maintains, or uses student personally identifiable information. &quot;School service&quot; 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. (C.R.S. § 22-16-103(7)(a))</td>
<td></td>
</tr>
<tr>
<td><strong>School service contract provider (contract provider)</strong></td>
<td>An entity, other than a public education entity, that enters into a formal, negotiated contract with a public education entity to provide a school service. (C.R.S. § 22-16-103(8))</td>
<td></td>
</tr>
<tr>
<td><strong>School service on-demand provider (on-demand provider)</strong></td>
<td>An entity, other than a public education entity, that provides a school service on occasion to a public education entity, subject to agreement by the public education entity, or an employee of the public education entity, to standard, non-negotiable terms and conditions of service established by the providing entity. (C.R.S. § 22-16-103(9))</td>
<td></td>
</tr>
<tr>
<td><strong>Student personally identifiable information</strong></td>
<td>Information that, alone or in combination, personally identifies an individual student or the student’s parent or family, and that is collected, maintained, generated, or inferred by a public education entity, either directly or through a school service, or by a school service contract provider or school service on-demand provider. (C.R.S. § 22-16-103(13))</td>
<td>Personally identifiable information includes, but is not limited to: (a) The student’s name; (b) the name of the student’s parent or other family members; (c) the address of the student or student’s family; (d) a personal identifier, such as the student’s social security number, student number, or biometric record; (e) other indirect identifiers, such as the student’s date of birth, place of birth, and mother’s maiden name; (f) other information that, alone or in combination, is linked to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or (g) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. (20 U.S.C. § 1232g)</td>
</tr>
</tbody>
</table>