

POLICIES, PLANS, AND OTHER MAJOR REQUIREMENTS OF THE STUDENT DATA PROTECTION ACT

Policies

- **53A-1-1404(1).** An LEA shall adopt policies to protect student data in accordance with the Student Data Protection Act and board rule, taking into account the specific needs and priorities of the LEA.
 - The required policies would likely address at least the following:
 - The LEA's collection, maintenance, use, storage, sharing, and deletion of student data;
 - The LEA's student data manager and the rules and requirements related to that position;
 - The LEA's data governance plan (the actual data governance plan could be separate from the policy, however);
 - The LEA's metadata dictionary (the actual metadata dictionary could be separate from the policy, however);
 - The LEA's external research review process for a request for data for the purpose of external research or evaluation ;
 - Student data ownership;
 - Notification in case of a release of personally identifiable student data due to a security breach; and
 - Requirements/process the LEA will follow in connection with sharing student data with third-party contractors.
 - The FERPA and/or student data policies adopted by LEAs prior to the enactment of the Student Data Protection Act likely contain some of the policy requirements described above, but not all. So, new or amended policies will need to be adopted by LEAs to comply with the requirements in the Student Data Protection Act.

Plans

- **53A-1-1404(3)(a).** An LEA shall create and maintain an LEA data governance plan.
 - 53A-1-1402(9) addresses what a data governance plan must include.

Other Major Requirements

- **53A-1-1404(2).** An LEA shall designate an individual to act as a student data manager to fulfill the responsibilities of a student data manager described in Section 53A-1-1409. If possible, an LEA shall designate the LEA's records officer as defined in Section 63G-2-103, as the student data manager.
- **53A-1-1404(3)(b).** An LEA shall create and maintain an LEA metadata dictionary.
 - 53A-1-1402(16) addresses the requirements of a metadata dictionary.
- **53A-1-1404(4).** An LEA shall establish an external research review process for a request for data for the purpose of external research or evaluation.
- **53A-1-1406(3).** Beginning with the 2017-18 school year, an education entity that collects student data into a cumulative record shall prepare and distribute to parents and students a student data disclosure statement. There are a variety of requirements in this Section with respect to the student

data disclosure statement, including that it be a stand-alone document, annually updated, and published on the education entity's website.

- **53A-1-1406(6).** Beginning with the 2017-18 school year, an education entity may collect a student's biometric identifier or biometric information into a cumulative record if the education entity provides to an adult student or a minor student's parent a biometric information disclosure statement that is separate from a student data disclosure statement. This Section describes what must be included in the biometric information disclosure statement.
- **53A-1-1409.** Beginning with the 2017-18 school year, an education entity may not share a student's personally identifiable student data if the personally identifiable student data is not shared in accordance with FERPA and the Student Data Protection Act. The responsibilities of school data managers and various requirements related to their management and sharing of personally identifiable student data is set forth in this Section.
- **53A-1-1410.** This Section provides a list of data privacy/security provisions an educational entity must include in contracts with third-party contractors. The provisions deal with a third-party's collection, use, storage, and sharing of student data. This Section contains a lot of requirements and rules regarding third-party contractor uses of student data.

ADA Compliant 03/08/2018