R277. Education, Administration.

R277-487. Public School Data Confidentiality and Disclosure.

R277-487-1. Authority and Purpose.

(1) This rule is authorized by:

(a) Utah Constitution Article X, Section 3, which vests general control and supervision over public education in the Board;

(b) Subsection 53E-3-401(4), which allows the Board to make rules to execute the Board's duties and responsibilities under the Utah Constitution and state law;

(c) Subsection 53E-9-302(1), which directs that the Board may make rules to establish student data protection standards for public education employees, student aides, and volunteers; and

(d) Subsection 53G-11-511(4), which directs that the Board may make rules to ensure the privacy and protection of individual evaluation data.

(2) The purpose of this rule is to:

(a) provide for appropriate review and disclosure of student performance data on state administered assessments as required by law;

(b) provide for adequate and appropriate review of student performance data on state administered assessments to professional education staff and parents of students;

(c) ensure the privacy of student performance data and personally identifiable student data, as directed by law; and

(d) provide for appropriate protection and maintenance of educator licensing data.

R277-487-2. Definitions.

(1) "Classroom-level assessment data" means student scores on state-required tests, aggregated in groups of more than 10 students at the classroom level or, if appropriate, at the course level, without individual student identifiers of any kind.

(2) "Comprehensive Administration of Credentials for Teachers in Utah Schools" or "CACTUS" means the electronic file maintained and owned by the Board on all licensed Utah educators, which includes information such as:

(a) personal directory information;

(b) educational background;

(c) endorsements;

(d) employment history; and

(e) a record of disciplinary action taken against the educator.

(3) "Confidentiality" refers to an obligation not to disclose or transmit information to unauthorized parties.

(4) “Cyber security framework” means:

(a) the cyber security framework developed by the Center for Internet Security found at http://www.cisecurity.org/controls/; or

(b) a IT security framework that is comparable to the cyber security framework described in Subsection (6)(a).

(5) "Data governance plan" has the same meaning as defined in Subsection 53E-9-301(6).

(6) “Destroy” means to remove data or a record:

(a) in accordance with current industry best practices; and

(b) rendering the data or record irretrievable in the normal course of business of an LEA or a third-party contractor.

(7) "Disclosure" includes permitting access to, revealing, releasing, transferring, disseminating, or otherwise communicating all or any part of any individual record orally, in writing, electronically, or by any other communication method.

(8) “Expunge” means to seal a record so as to limit its availability to all except authorized individuals.

(9) "Enrollment verification data" includes:

(a) a student’s birth certificate or other verification of age;

(b) verification of immunization or exemption from immunization form;

(c) proof of Utah public school residency;

(d) family income verification; or

(e) special education program information, including:

(i) an individualized education program;

(ii) a Section 504 accommodation plan; or

(iii) an English language learner plan.

(10) "FERPA" means the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g, and its implementing regulations found at 34 C.F.R., Part 99.

(11) "LEA" includes, for purposes of this rule, the Utah Schools for the Deaf and the Blind.

(12) "Metadata dictionary" means any tool, document, or display that meets the requirements of Subsection 53E-9-301(11).

(13) "Personally identifiable student data" has the same meaning as defined in Subsection 53E-9-301(14) and 34 CFR 99.3.

(14) “Significant data breach” means a data breach where:

(a) an intentional data breach successfully compromises student records;

(b) a large number of student records are compromised;

(c) sensitive records are compromised, regardless of number; or

(d) a data breach an LEA deems to be significant based on the surrounding circumstances.

(15) "Student performance data" means data relating to student performance, including:

(a) data on state, local and national assessments;

(b) course-taking and completion;

(c) grade-point average;

(d) remediation;

(e) retention;

(f) degree, diploma, or credential attainment; and

(g) enrollment and demographic data.

(16) "Third party contractor" has the same meaning as defined in Subsection 53E-9-301(23).

R277-487-3. Data Privacy and Security Policies.

(1) By October 1 annually, each LEA shall provide the Superintendent with the following information:

(a) the name and contact information for the LEA’s designated data manager and information security officer;

(b) the LEA's data governance plan;

(c) the LEA's annual notification of FERPA rights, as described in 34 CFR 99.7;

(d) the LEA's directory information notice, as described in 34 CFR 99.37;

(e) the LEA's student data collection notice, as described in Subsection 53E-9-305(2);

(f) the LEA's metadata dictionary; and

(g) evidence that the LEA has implemented a cyber security framework.

(2) An LEA shall ensure that school enrollment verification data, student performance data, and personally identifiable student data are collected, maintained, and transmitted:

(a) in a secure manner; and

(b) consistent with sound data collection and storage procedures based on the LEA's cyber security framework.

(3) An LEA shall report all significant data breaches of student data either by the LEA or by third parties to the Superintendent within ten business days of the initial discovery of the significant data breach.

(4) All public education employees, aides, and volunteers shall maintain appropriate confidentiality pursuant to federal, state, local laws, and LEA policies created in accordance with this section, with regard to student performance data and personally identifiable student data.

(5) An employee, aide, or volunteer may not share, disclose, or disseminate passwords for electronic maintenance of:

(a) student performance data; or

(b) personally identifiable student data.

(6) A public education employee licensed under Section 53E-6-201 may only access or use student information and records if the public education employee accesses the student information or records consistent with the educator's obligations under Rule R277-217.

(7) The Board may discipline a licensed educator in accordance with licensing discipline procedures if the educator violates this Rule R277-487.

(8) In accordance with the LEA's data governance plan, each LEA shall annually

provide a training regarding the confidentiality of student data to any employee with access to education records as defined in FERPA.

R277-487-4. Retention of Student Data.

(1) An LEA shall classify all student data collected in accordance with Section 63G-2-604.

(2) An LEA shall retain and dispose of all student data in accordance with an approved retention schedule.

(3) If no existing retention schedule governs student disciplinary records collected by an LEA:

(a) An LEA may propose to the State Records Committee a retention schedule of up to one year if collection of the data is not required by federal or state law or Board rule; or

(b) An LEA may propose to the State Records Committee a retention schedule of up to three years if collection of the data is required by federal or state law or Board rule, unless a longer retention period is prescribed by federal or state law or Board rule.

(4) An LEA's retention schedules shall take into account the LEA's administrative need for the data.

(5) Unless the data requires permanent retention, an LEA's retention schedules shall require destruction or expungement of student data after the administrative need for the data has passed.

(6) A parent or adult student may request that an LEA amend, expunge, or destroy any record not subject to a retention schedule under Section 63G-2-604, and believed to be:

(a) inaccurate;

(b) misleading; or

(c) in violation of the privacy rights of the student.

(7) An LEA shall process a request under Subsection (6) following the same procedures outlined for a request to amend a student record in 34 CFR Part 99, Subpart C.

R277-487-5. CACTUS Data.

(1) The Board maintains information on all licensed Utah educators in CACTUS, including information classified as private, controlled, or protected under GRAMA.

(2) The Superintendent shall open a CACTUS file for a licensed Utah educator when the individual initiates a Board background check.

(3) Authorized Board staff may update CACTUS data as directed by the Superintendent.

(4) Authorized LEA staff may change demographic data and update data on educator assignments in CACTUS for the current school year only.

(5) A licensed individual may view his own personal data, but may not change or add data in CACTUS except under the following circumstances:

(a) A licensee may change the licensee's contact and demographic information at any time;

(b) An employing LEA may correct a current educator's assignment data on behalf of a licensee; and

(c) A licensee may petition the Board for the purpose of correcting any errors in the licensee's CACTUS file.

(6) The Superintendent shall include an individual currently employed by a public or private school under a letter of authorization or as an intern in CACTUS.

(7) The Superintendent shall include an individual working in an LEA as a student teacher in CACTUS.

(8) The Superintendent shall provide training and ongoing support to authorized CACTUS users.

(9) For employment or assignment purposes only, authorized LEA staff members may:

(a) access data on individuals employed by the LEA; or

(b) view specific limited information on job applicants if the applicant has provided the LEA with a CACTUS identification number.

(10) CACTUS information belongs solely to the Board.

(g) The Superintendent may release data within CACTUS in accordance with the provisions of Title 63G, Chapter 2, Government Records Access and Management Act.

R277-487-6. Educator Evaluation Data.

(1)(a) The Superintendent may provide classroom-level assessment data to administrators and teachers in accordance with federal and state privacy laws.

(b) A school administrator shall share information requested by parents while ensuring the privacy of individual personally identifiable student data and educator evaluation data.

(2) A school, LEA, the Superintendent, and the Board shall protect individual educator evaluation data.

(3) An LEA shall designate employees who may have access to educator evaluation records.

(4) An LEA may not release or disclose student assessment information that reveals educator evaluation information or records.

(5) An LEA shall train employees in the confidential nature of employee evaluations and the importance of securing evaluations and records.

R277-487-7. Application to Third Parties.

(1) A third-party contractor shall protect student personally identifiable information against unauthorized access and redisclosure, both physical and digital.

(2) A third-party contractor shall have policies in place that follow reasonably industry best practices and adequately address the protection of student personally identifiable information.

(3) A third-party contractor shall develop and document an information security program.

(4) A third-party contract shall informn an LEA or the Superintendent of the precautions taken regarding the maintenance and protection of student personally identifiable information.

(5) For the purposes of meeting the audit requirements of a contract subject to Subsection 53E-9-309(2)(e), a third-party contractor may:

(a) provide an LEA or the Superintendent a self-assessment of their compliance with the contract and the effectiveness of the information security program described in

Subsection (3);

(b) provide responses to a questionnaire provided by the LEA or Superintendent;

(c) provide a report of an industry-recognized privacy and security audit, such as an SOC2 or SOC3; or

(d) submit to an onsite audit, if agreed upon by the third-party contract and the LEA or Superintendent.

R277-487-8. Sharing Data With the Utah Registry of Autism and Developmental Disabilities.

(1) The Superintendent shall share personally identifiable student data with the Utah Registry of Autism and Developmental Disabilities as required by Subsection 53E-9-308(6)(b) through a written agreement designating the Utah Registry of Autism and Developmental Disabilities as the authorized representative of the Board for the purpose of auditing and evaluating federal and state supported education programs that serve students with autism and other developmental disabilities.

(2) The agreement required by Subsection (1) shall include a provision that:

(a) the Utah Registry of Autism and Developmental Disabilities may not use personally identifiable student data for any purpose not specified in the agreement;

(b) the Utah Registry of Autism and Developmental Disabilities shall flag all student personally identifiable data received from the Board to:

(i) ensure that the data is not used for purposes not covered by the agreement; and

(ii) allow the Superintendent access to the data for auditing purposes;

(c) the Utah Registry of Autism and Developmental Disabilities may redisclose de-identified data if:

(i) the de-identification is in accordance with HIPAA's safe harbor standard;

(ii) the de-identification is in accordance with Board rule; and

(iii) the Utah Registry of Autism and Development Disabilities annually provides the Superintendent with a description and the results of all projects and research undertaken using de-identified student data; and

(d) the Utah Registry of Autism and Developmental Disabilities shall allow an

audit that meets the requirements of Subsection R277-487-7(5) conducted by the Superintendent to monitor for compliance with this rule no less than once per year.

(3) The Superintendent shall maintain a record of all personally identifiable student data shared with the Utah Registry of Autism and Developmental Disabilities in accordance with 34 C.F.R. 99.32.

(4)(a) A parent of a child whose personally identifiable student data was shared with the Utah Registry of Autism and Developmental Disabilities has the right to access the exact records disclosed.

(b) A parent identified in Subsection (4)(a) has the right to contest and seek to amend, expunge, or destroy any data that is inaccurate, misleading, or otherwise in violation of the privacy rights of the student.

R277-487-9. Data Security and Privacy Training for Educators.

(1) The Superintendent shall develop a student and data security and privacy training for educators.

(2) Beginning in the 2018-19 school year, an educator shall complete the training developed in accordance with Subsection (1) as a condition of re-licensure.

KEY: students, records, confidentiality, privacy
Date of Enactment or Last Substantive Amendment: November 8, 2019
Notice of Continuation: November 14, 2014
Authorizing, and Implemented, or Interpreted Law: Art X Sec 3; 53E-9-302; 53E-3-401; 53G-11-511.