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;

(d) provide an online education survey conducted with public funds for Board review and approval; and

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

R277-487-2. Definitions.

(1) "Association" has the same meaning as that term is defined in Subsection 53-7-1101(3).

(2) "Chief Privacy Officer" means a Board employee designated by the Board as primarily responsible to:

(a) oversee and carry out the responsibilities of this rule; and

(b) direct the development of materials and training about student and public education employee privacy standards for the Board and LEAs, including:

(i) FERPA; and

(ii) the Utah Student Data Protection Act, Title 53E, Chapter 9, Part 3.

(3) "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.

(4) "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.

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

(6) “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).

(7) "Data governance plan" has the same meaning as defined in Subsection 53E-9-301(7).

(8) "Data security protections" means protections developed and initiated by the Superintendent that protect, monitor and secure student, public educator and public education employee data as outlined and identified in FERPA and Sections 63G-2-302 through 63G-2-305.

(9) “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.

(10) "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.

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

(12) "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.

(13) "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.

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

(15) "Metadata dictionary" has the same meaning as defined in Subsection 53E-9-301(14).

(16) "Personally identifiable student data" has the same meaning as defined in Subsection 53E-9-301(14).

(17) “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.

(18) "Student data advisory groups" has the same meaning as described in Subsection 53E-9-302(3).

(19) "Student data manager” means the individual at the LEA level who:

(a) is designated as the student data manager by an LEA under Section 53E-9-303;

(b) authorizes and manages the sharing of student data;

(c) acts as the primary contact for the Chief Privacy Officer;

(d) maintains a list of persons with access to personally identifiable student data; and

(e) is in charge of providing annual LEA staff and volunteer training on data privacy.

(20) "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.

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

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

(1) The Superintendent shall develop resource materials for LEAs to train employees, aides, and volunteers of an LEA regarding confidentiality of personally identifiable student data and student performance data.

(2) The Superintendent shall make the materials developed in accordance with Subsection (1) available to each LEA.

(3) An LEA or public school may not be a member of or pay dues to an association that is not in compliance with:

(a) FERPA;

(b) Title 53E, Chapter 9, Part 3, Student Data Protection Act;

(c) Title 53E, Chapter 9, Part 2, Utah Family Educational Rights and Privacy Act; and

(d) this Rule R277-487.

(4) An LEA shall comply with Title 53E, Chapter 9, Part 3, Student Data Protection Act.

(5) An LEA shall comply with Section 53E-9-204.

(6) An LEA is responsible for the collection, maintenance, and transmission of

student data.

(7) 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, established by the LEA.

(8) An LEA may contract with a third party contractor to collect, maintain, and have access to school enrollment verification data or other student data if:

(a) the third party contractor meets the definition of a school official under 34 C.F.R. 99.31(a)(1)(i)(B); and

(b) the contract between the LEA and the third party contractor includes the provisions required by Subsection 53E-9-309(2).

(9) An LEA shall publicly post the LEA's definition of directory information, as defined in FERPA, and describe how a student data manager may share personally identifiable information that is directory information.

(10) An LEA shall provide the Superintendent with a copy or link to the LEA's directory information definition by October 1 annually.

(11) By October 1 annually, an LEA shall enter all student data elements shared with third parties into the Board's metadata dictionary.

(12) 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.

(13) An LEA shall provide the Superintendent with a copy or link to the LEA's data governance plan by October 1 annually.

(14) An LEA shall provide the Superintendent with the following information by October 1 annually:

(a) evidence that the LEA has implemented a cyber security framework; and

(b) the name and contacted information for the LEA's designated Information Security Officer.

(15) All public education employees, aides, and volunteers in public schools shall become familiar with federal, state, and local laws regarding the confidentiality of student

performance data and personally identifiable student data.

(16) 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.

(17) 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.

(18) 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 R277-515.

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

(20) An 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 Transparency.

(1) The Superintendent shall recommend policies for Board approval and model policies for LEAs regarding student data systems.

(2) A policy prepared in accordance with Subsection (1) shall include provisions regarding:

(a) accessibility by parents, students, and the public to student performance data;

(b) authorized purposes, uses, and disclosures of data maintained by the Superintendent or an LEA;

(c) the rights of parents and students regarding their personally identifiable information under state and federal law;

(d) parent, student, and public access to information about student data privacy and the security safeguards that protect the data from unauthorized access and use; and

(e) contact information for parents and students to request student and public school information from an LEA consistent with the law.

R277-487-6 Responsibilities of Chief Privacy Officer.

(1) The Chief Privacy Officer:

(a) may recommend legislation, as approved by the Board, for additional data

security protections and the regulation of use of the data;

(b) shall supervise regular privacy and security compliance audits, following initiation by the Board;

(c) shall have responsibility for identification of threats to data privacy protections;

(d) shall develop and recommend policies to the Board and model policies for LEAs for:

(i) protection of personally identifiable student data;

(ii) consistent wiping or destruction of devices when devices are discarded by public education entities; and

(iii) appropriate responses to suspected or known breaches of data security protections;

(e) shall conduct training for Board staff and LEAs on student privacy; and

(f) shall develop and maintain a metadata dictionary as required by Section 53E-9-302.

R277-487-7. Prohibition of Public Education Data Use for Marketing.

Data maintained by the state, a school district, school, or other public education agency or institution in the state, including data provided by contractors, may not be sold or used for marketing purposes, or targeted advertising as defined in Subsection 53E-9-301(22) except with regard to authorized uses of directory information not obtained through a contract with an educational agency or institution.

R277-487-8. Public Education Research Data.

(1) The Superintendent may provide limited or extensive data sets for research and analysis purposes to qualified researchers or organizations.

(2) The Superintendent shall use reasonable methods to qualify researchers or organizations to receive data, such as evidence that a research proposal has been approved by a federally recognized Institutional Review Board or "IRB.".

(3) The Superintendent may post aggregate de-identified student assessment data to the Board website.

(4) The Superintendent shall ensure that personally identifiable student data is protected.

(5) The Superintendent:

(a) is not obligated to fill every request for data and shall establish procedures to determine which requests will be filled or to assign priorities to multiple requests;

(b) may give higher priority to requests that will help improve instruction in Utah's public schools; and

(c) may charge a fee to prepare data or to deliver data, particularly if the preparation requires original work.

(6) A researcher or organization shall provide a copy of the report or publication produced using Board data to the Superintendent at least 10 business days prior to the public release.

(7) Requests for personally identifiable student data that may only be provided in accordance with Section 53E-9-308 and FERPA, and may include:

(a) student data that are de-identified, meaning that a reasonable person in the school community who does not have personal knowledge of the relevant circumstances could not identify student(s) with reasonable certainty;

(b) agreements with recipients of student data where recipients agree not to report or publish data in a manner that discloses students' identities; or

(c) release of student data, with appropriate binding agreements, for state or federal accountability or for the purpose of improving instruction to specific student subgroups.

(8) Recipients of Board research data shall sign a confidentiality agreement, if required by the Superintendent.

(9) Either the Board or the Superintendent may commission research or may approve research requests.

(10) Request for records under Title 63G, Chapter 2, Government Records Access and Management Act, are not subject to this Section R277-487-8

R277-487-9. 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.

R277-487-10. 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.

R277-487-11. Application to Third Parties.

(1) The Board and LEAs shall set policies that govern a third party contractor's access to personally identifiable student data and public school enrollment verification data consistent with Section 53E-9-301, et seq.

(2) An LEA may release personally identifiable student data and public school enrollment verification data to a third party contractor if:

(a) the release is allowed by, and released in accordance with, Section 53E-9-308, FERPA, and FERPA's implementing regulations; and

(b) the LEA complies with the requirements of Subsection R277-487-3(6).

(4) All Board contracts shall include sanctions for contractors or third party providers who violate provisions of state policies regarding unauthorized use and release of student and employee data.

(5) The Superintendent shall recommend that LEA policies include sanctions for contractors who violate provisions of federal or state privacy law and LEA policies regarding unauthorized use and release of student and employee data.

R277-487-12. 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 HIPPA'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 on-site audit 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.

R277-487-13. Annual Reports by Chief Privacy Officer.

(1) The Chief Privacy Officer shall submit to the Board an annual report regarding student data.

(2) The public report shall include:

(a) information about the implementation of this rule;

(b) information about the approved research studies using personally identifiable student information and data;

(c) identification of significant threats to student data privacy and security;

(d) a summary of data system audits; and

(e) recommendations for further improvements specific to student data security and the systems that are necessary for accountability in Board rules or legislation.

R277-487-14. Data Security and Privacy Training for Educators.

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

(2) The Superintendent shall make the training developed in accordance with Subsection (1) available through UEN.

(3) 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
Date of Enactment or Last Substantive Amendment: 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.