

1 **R277. Education, Administration.**

2 **R277-487. Public School Data Confidentiality and Disclosure.**

3 **R277-487-1. Authority and Purpose.**

4 (1) This rule is authorized by:

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

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

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

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

14 (2) The purpose of this rule is to:

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

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

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

21 (d) provide for appropriate protection and maintenance of educator licensing data.
22

23 **R277-487-2. Definitions.**

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

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

- 30 (a) personal directory information;
- 31 (b) educational background;
- 32 (c) endorsements;
- 33 (d) employment history; and
- 34 (e) a record of disciplinary action taken against the educator.

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

37 (4) "Cyber security framework" means:

- 38 (a) the cyber security framework developed by the Center for Internet Security
39 found at <http://www.cisecurity.org/controls/>; or
- 40 (b) a IT security framework that is comparable to the cyber security framework
41 described in Subsection (6)(a).

42 (5) "Data governance plan" has the same meaning as defined in Subsection [53E-](#)
43 [9-301\(6\)](#).

44 (6) "Destroy" means to remove data or a record:

- 45 (a) in accordance with current industry best practices; and
- 46 (b) rendering the data or record irretrievable in the normal course of business of an
47 LEA or a third-party contractor.

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

51 (8) "Expunge" means to seal a record so as to limit its availability to all except
52 authorized individuals.

53 (9) "Enrollment verification data" includes:

- 54 (a) a student's birth certificate or other verification of age;

- 55 (b) verification of immunization or exemption from immunization form;
- 56 (c) proof of Utah public school residency;
- 57 (d) family income verification; or
- 58 (e) special education program information, including:
- 59 (i) an individualized education program;
- 60 (ii) a Section 504 accommodation plan; or
- 61 (iii) an English language learner plan.
- 62 (10) "FERPA" means the Family Educational Rights and Privacy Act of 1974, 20
63 U.S.C. 1232g, and its implementing regulations found at 34 C.F.R., Part 99.
- 64 (11) "LEA" includes, for purposes of this rule, the Utah Schools for the Deaf and the
65 Blind.
- 66 (12) "Metadata dictionary" means any tool, document, or display that meets the
67 requirements of Subsection [53E-9-301](#)(11).
- 68 (13) "Personally identifiable student data" has the same meaning as defined in
69 Subsection [53E-9-301](#)(14) and 34 CFR 99.3.
- 70 (14) "Significant data breach" means a data breach where:
- 71 (a) an intentional data breach successfully compromises student records;
- 72 (b) a large number of student records are compromised;
- 73 (c) sensitive records are compromised, regardless of number; or
- 74 (d) a data breach an LEA deems to be significant based on the surrounding
75 circumstances.
- 76 (15) "Student performance data" means data relating to student performance,
77 including:
- 78 (a) data on state, local and national assessments;
- 79 (b) course-taking and completion;
- 80 (c) grade-point average;
- 81 (d) remediation;
- 82 (e) retention;

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

84 (g) enrollment and demographic data.

85 (16) "Third party contractor" has the same meaning as defined in Subsection [53E-](#)
86 [9-301](#)(23).

87 (17) "Student Contact Information" means information collected for student directory
88 purposes that is limited to:

89 (a) student name

90 (b) mailing address

91 (c) grade level

92 (18) "UTREx" has the same meaning as defined in Subsection [R277-484-2](#)(16).

93

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

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

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

99 (b) the LEA's data governance plan;

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

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

102 (e) the LEA's student data collection notice, as described in Subsection [53E-9-](#)
103 [305](#)(2);

104 (f) the LEA's metadata dictionary; and

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

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

109 (a) in a secure manner; and

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

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

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

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

121 (a) student performance data; or

122 (b) personally identifiable student data.

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

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

129 (8) In accordance with the LEA's data governance plan, each LEA shall annually
130 provide a training regarding the confidentiality of student data to any employee with
131 access to education records as defined in FERPA.

132

133 **R277-487-4. Retention of Student Data.**

134 (1) An LEA shall classify all student data collected in accordance with Section [63G-](#)
135 [2-604](#).

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

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

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

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

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

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

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

154 (a) inaccurate;

155 (b) misleading; or

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

157 (7) An LEA shall process a request under Subsection (6) following the same
158 procedures outlined for a request to amend a student record in 34 CFR Part 99, Subpart C.
159

160 **R277-487-5. CACTUS Data.**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

188 (10) CACTUS information belongs solely to the Board.

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

191

192 **R277-487-6. Educator Evaluation Data.**

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

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

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

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

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

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

206

207 **R277-487-7. Application to Third Parties.**

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

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

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

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

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

220 (a) provide an LEA or the Superintendent a self-assessment of their compliance
221 with the contract and the effectiveness of the information security program described in
222 Subsection (3);

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

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

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

228

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

231 (1) The Superintendent shall share personally identifiable student data with the
232 Utah Registry of Autism and Developmental Disabilities as required by Subsection [53E-9-](#)
233 [308\(6\)\(b\)](#) through a written agreement designating the Utah Registry of Autism and
234 Developmental Disabilities as the authorized representative of the Board for the purpose of
235 auditing and evaluating federal and state supported education programs that serve students
236 with autism and other developmental disabilities.

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

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

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

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

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

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

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

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

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

251 (d) the Utah Registry of Autism and Developmental Disabilities shall allow an audit
252 that meets the requirements of Subsection R277-487-7(5) conducted by the Superintendent
253 to monitor for compliance with this rule no less than once per year.

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

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

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

263

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

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

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

269

270 **R277-487-10. Advertising Public School Enrollment Options.**

271 (1) An LEA shall establish an opt in process for sharing student contact information
272 with other LEAs for the purpose of advertising public school enrollment options.

273 (2) An LEA shall send student contact information and the parent opt in indicator to
274 the Superintendent through UTREx.

275 (3) An LEA may request student contact information from the Superintendent.

276 (4) The Superintendent shall, upon request from an LEA, share the requested
277 student contact information where the opt in indicator is present with the requesting LEA.

278 (5) An LEA may not use student contact information received under Subsection (5)
279 for any purpose other than the advertisement of public school enrollment options.

280 (6) The Superintendent may only share student contact information with a Utah LEA.

281

282 **KEY: students, records, confidentiality, privacy**

283 **Date of Enactment or Last Substantive Amendment: November 8, 2019**

284 **Notice of Continuation: September 9, 2019**

285 **Authorizing, and Implemented or Interpreted Law: [Art X Sec 3](#); [53E-9-302](#); [53E-3-](#)**
286 **[401](#); [53G-11-511](#)**