

SB0267S02 compared with SB0267

~~{Omitted text}~~ shows text that was in SB0267 but was omitted in SB0267S02

inserted text shows text that was not in SB0267 but was inserted into SB0267S02

DISCLAIMER: This document is provided to assist you in your comparison of the two bills. Sometimes this automated comparison will NOT be completely accurate. Therefore, you need to read the actual bills. This automatically generated document could contain inaccuracies caused by: limitations of the compare program; bad input data; or other causes.

1 **Software in Education Amendments**
2026 GENERAL SESSION
STATE OF UTAH
Chief Sponsor: Kirk A. Cullimore
House Sponsor:



2
3 **LONG TITLE**

4 **General Description:**

5 This bill creates certain requirements and accountability procedures regarding a student's
6 use of software in a public school.

7 **Highlighted Provisions:**

8 This bill:

- 9 ▶ defines terms;
- 10 ▶ requires the State Board of Education to:
- 11 • create a statewide digital privacy agreement for educational software;
 - 12 • ensure that all software used in a public school is executed under the statewide digital
13 privacy agreement and academically effective;
 - 14 • create a master list for software used in public schools;
 - 15 • create a process for a vendor to certify that the vendor's software is academically
16 effective;
 - 15 • create a list of approved software;
 - 16 • {~~independently~~} verify software as academically effective;

SB0267 compared with SB0267S02

- 17 • enforce compliance with the requirements of this section through periodic audits;
- 18 • create a process for a parent to submit a complaint; and
- 19 • create rules to implement the requirements of this section;
- 22 ▶ **creates exceptions for the statewide digital privacy agreement;**
- 20 ▶ requires a local education agency (LEA), the Utah Education and Telehealth Network, and the State Board of Education to:
- 22 • execute the statewide digital privacy agreement for all software contracts; and
- 23 • verify certain software is academically effective;
- 27 ▶ **requires the use of a digital privacy agreement for administrative software;**
- 28 ▶ **allows a vendor to offer educational software to a contracting entity on a provisional basis;**
- 24 ▶ requires an LEA to notify parents of all software a public school uses during the school year;
- 26 ▶ requires the state board to consult with the Office of the Attorney General; and
- 27 ▶ {requires a vendor to:}
- 28 • requires a vendor to execute the statewide digital privacy agreement for all software contracts with a contracting entity {~~and~~} .
- 30 • {~~demonstrate that the vendor's software is academically effective.~~}

Money Appropriated in this Bill:

35 None

Other Special Clauses:

37 This bill provides a special effective date.

Utah Code Sections Affected:

39 ENACTS:

40 **53G-7-1401** , Utah Code Annotated 1953

41 **53G-7-1402** , Utah Code Annotated 1953

42 **53G-7-1403** , Utah Code Annotated 1953

43 **53G-7-1404** , Utah Code Annotated 1953

44 **53G-7-1405** , Utah Code Annotated 1953

45 **53G-7-1406** , Utah Code Annotated 1953

46 **53G-7-1407 , Utah Code Annotated 1953**

48 *Be it enacted by the Legislature of the state of Utah:*

SB0267 compared with SB0267S02

49 Section 1. Section 1 is enacted to read:

51 **53G-7-1401. General provisions -- Definitions.**

14. Software Policy

As used in this part:

53 (1) "Academic progress" means advancement toward mastery of state academic standards through practice, application, feedback, or demonstration of knowledge or skill.

49 (1){(2)} "Academically effective" means software that:

50 (a) is designed to {support} provide support, or enable student active learning, skill development, or academic {~~performance~~} progress in the intended subject area ~~{, as supported by:} ;~~

52 {(i) ~~{peer-reviewed research on similar educational interventions;}~~}

53 {(ii) ~~{evidence of positive outcomes in comparable educational settings;}~~}

54 {(iii) ~~{sound pedagogical principles recognized in the field of education; or}~~}

55 {(iv) ~~{independent evaluation demonstrating educational value;}~~}

56 (b) where applicable, aligns with the public education core standards described in Section 53E-4-202 ~~{, where applicable to the software's educational purpose} ;~~

58 {(e) ~~{demonstrates instructional value through;}~~}

59 {(i) ~~{supporting differentiated instruction;}~~}

60 {(ii) ~~{providing formative assessment and feedback;}~~}

61 {(iii) ~~{engaging students in active learning;}~~}

62 {(iv) ~~{supplementing teacher instruction; or}~~}

63 {(v) ~~{other recognized effective educational practices;}~~}

64 (d){(c)} does not employ design features that primarily:

65 {(i) ~~{distract from learning objectives;}~~}

66 {(ii) ~~{prioritize entertainment over educational content; or}~~}

61 (i) interfere with active learning; or

67 (iii){(ii)} undermine teacher instructional authority; and

68 (e){(d)} ~~{has potential to produce positive}~~ contributes to or enables measurable academic ~~{outcomes}~~ progress or skill development when used ~~{appropriately in a classroom setting as part of a comprehensive instructional program}~~ as intended.

65 (3) "Active learning" means instruction that requires a student to engage in cognitive processes including analyzing, reasoning, practicing, or creating to understand or apply knowledge or skills.

SB0267 compared with SB0267S02

- 70 (2){(4)}
- (a) "Addictive design feature" means a feature or component of a digital or online product that encourages or increases a student's frequency, time spent, or engagement with the product.
- 73 (b) "Addictive design feature" includes the following features:
- 72 (i) infinite scroll;
- 74 (i){(ii)} ~~{infinite scroll or}~~ autoplay that continues beyond the educational task or lesson;
- 75 (ii){(iii)} points, badges, or other gamification rewards tied ~~{primarily}~~ to time spent on the product rather than learning ~~{achievement}~~ objectives or academic progress;
- 77 (iii){(iv)} persistent notifications prompting re-engagement when the product is not actively in use, unless ~~{directly related to assigned schoolwork or teacher communication;}~~ :
- 78 (A) a teacher initiates the notification; and
- 79 (B) the notification is directly related to assigned schoolwork;
- 80 (iv){(v)} personalized recommendation systems designed to maximize time-on-platform rather than learning outcomes; or
- 82 (v){(vi)} engagement metrics, streaks, or social comparison features designed to create fear of missing out or compulsive checking behavior.
- 84 (c) "Addictive design feature" does not include{:} a:
- 85 ~~{(i) {progress indicators or achievement recognition tied to demonstrated learning;}}~~
- 86 (ii){(i)} ~~{recommendations}~~ recommendation of next lessons or learning activities based on curriculum progression or mastery of prerequisites;
- 88 (iii){(ii)} ~~{notifications}~~ notification about ~~{upcoming assignments}~~ a teacher-assigned or course-required assignment, ~~{deadlines}~~ deadline, or teacher feedback; or
- 89 (iv){(iii)} ~~{features}~~ feature that ~~{encourage productive academic engagement}~~ encourages active learning rather than passive consumption.
- 90 (5) "Administrative software" means software that a contracting entity uses solely for administrative, operational, or other non-instructional functions of the contracting entity.
- 91 (3){(6)} "Clickstream data" means data an LEA or third-party provider collects from a student's use of an online service, application, or device that records the student's navigation or sequence of actions.
- 94 (4){(7)} "Contracting entity" means the following entities if that entity contracts with a vendor for software:
- 96 (a) an LEA;

SB0267 compared with SB0267S02

- 97 (b) the state board;~~or~~
- 98 (c) UETN~~{;or}~~.
- 99 ~~{(d) {any other entity receiving state funds.}}~~
- 100 (5){(8)} "Digital privacy agreement" means a contract between a contracting entity and a digital provider that:
- 102 (a) ensures compliance with Title 53E, Chapter 9, Student Privacy and Data Protection; and
- 104 (b) governs access, use, protection, retention, and disclosure of student data.
- 105 (6){(9)}
- (a) "Educational purpose" means a purpose directly related to:
- 106 (i) student instruction;
- 107 (ii) assessment of a student; or
- 108 (iii) school operations necessary for instruction of a student.
- 109 (b) "Educational purpose" does not include:
- 110 (i) marketing;
- 111 (ii) advertising;
- 112 (iii) behavioral profiling; or
- 113 (iv) any other commercial purpose.
- 114 ~~{(7) {"Independently verified" means software that an impartial third party, with no financial or contractual relationship with the vendor and with demonstrated expertise appropriate to the type of software, checks for:}}~~
- 117 ~~{(a) {safety;}}~~
- 118 ~~{(b) {effectiveness; and}}~~
- 119 ~~{(c) {compliance with the requirements of this section.}}~~
- 120 (8){(10)} ~~{"Instructional }~~ "Educational software" means software that ~~{is safe, legal, and effective because the software is }~~:
- 115 (a) serves an educational purpose;
- 116 (b) is designed for student instruction, assessment, or instructional support;
- 122 (a){(c)} ~~{part of a }~~ is executed under the statewide digital privacy agreement; and
- 123 (b){(d)} is verified for academic effectiveness in accordance with the requirements of this section.
- 120

SB0267 compared with SB0267S02

- 124 (11) "Independently verified" means the characteristic of software that an impartial third party with
125 demonstrated expertise appropriate to the software type, whom the vendor does not own, control or
126 direct, and whose compensation does not depend on the evaluation outcome, evaluates for:
- 127 (a) academic effectiveness; and
128 (b) compliance with the requirements of this part.
- 129 (12) "Internet service provider" means the same as that term is defined in Section 76-5c-401.
- 130 (13) "Passive consumption" means receiving information through viewing, listening, or browsing
131 without requiring the student to engage in cognitive processing necessary to analyze, apply, or
132 create knowledge or skills.
- 133 (9){(14)} "School-issued device" means any electronic hardware device an LEA provides to a student
134 for educational use.
- 135 (15) "Skill development" means the acquisition or improvement of academic abilities or competencies
136 necessary to perform a task aligned to state academic standards, including guided practice,
137 modeling, or feedback.
- 138 (10){(16)}
- 139 (a) "Software" means any application, web-based service, plug-in, or other code-based product,
140 regardless of whether the application is free or for purchase, that:
- 141 (i) runs on or is accessible from a school-issued device {~~or from a student-owned device that the~~
142 ~~student uses for the student's education~~} ; and
- 143 (ii) an LEA assigns, requires, recommends, installs, or otherwise makes available for student use in
144 connection with classroom instruction, including through a school-issued account or identity,
145 regardless or whether the software is accessible on a school-issued or student-owned device.
- 146 (b) "Software" includes software an individual uses during school hours in connection with school-
147 related purposes for:
- 148 (i) instruction;
149 (ii) assessment;
150 (iii) communication;
151 (iv) collaboration;or
152 (v) enrichment{~~or~~};
153 {~~(vi) {recreation.}~~}
- 154 (c) "Software" does not include physical, electronic hardware.

SB0267 compared with SB0267S02

- 142 (11){(17)} "Statewide digital privacy agreement" means the digital privacy agreement the state board
creates in accordance with Section 53G-7-1402.
- 144 (12){(18)}
- (a) "Student data" means the same as that term is defined in Section 53E-9-301.
- 145 (b) "Student data" includes a student's:
- 146 {~~(i) {personally identifiable information;}~~}
- 154 (i) personal data as that term is defined in Section 13-61-101;
- 147 (ii) metadata, device identifiers, and clickstream data;
- 148 (iii) behavioral, engagement, or usage data; and
- 149 (iv) information a software collects, generates, or infers in the course of student use.
- 150 (13){(19)} "Sub-processor" means a third-party vendor or service that a primary data processor engages
to process personal data on the processor's behalf.
- 160 (20)
- (a) "Telecommunications carrier" means an entity that provides transmission, routing, or connectivity
services for digital communications, including wireless, broadband, or data transport services,
without modifying the content of communications.
- 164 (b) "Telecommunications carrier" includes an internet service provider.
- 152 (14){(21)} "Utah Education and Telehealth Network" or "UETN" means the same as that term is
defined in Section 53H-4-213.1.
- 167 (22)
- 154 (15){(a)} "Vendor" means an entity that provides software, digital tools, digital services, or related
technology to a contracting entity for student use, whether free or paid.
- 169 (b) "Vendor" does not include:
- 170 (i) a telecommunications carrier; or
- 171 (ii) an internet service provider.
- 156 (16){(23)} "Voice-print" means a digital representation of an individual's voice that a person creates,
derives, or uses to identify or authenticate the individual.
- 174 Section 2. Section 2 is enacted to read:
- 175 **53G-7-1402. Statewide digital privacy agreement-- Exceptions.**
- The state board shall create a form statewide digital privacy agreement, before July 1, 2027, that:
- 161

SB0267 compared with SB0267S02

- (1){(a)} governs student use of educational software and digital services in a public {schools;} school
for:
- 180 (i) kindergarten through grade 6; and
181 (ii) core standards, described in Section 53E-4-202, in grades 7 through 12;
- 162 (2){(b)} complies with the requirements of Title 53E, Chapter 9, Student Privacy and Data Protection,
including:
- 164 (a){(i)} data minimization;
165 (b){(ii)} prohibitions on {targeted-} advertising{:} or promotional content directed at a student,
including:
- 186 (A) advertising products or services to a student while the student is using educational software;
188 (B) allowing a third-party to advertise a product or a service to a student; and
189 (C) the inclusion of advertising or promotional content within educational software accessible to a
student;
- 166 (c){(iii)} limits on secondary data use;
167 (d){(iv)} security safeguards;
168 (e){(v)} breach notifications;
169 (f){(vi)} data retention and deletion requirements; and
170 (g){(vii)} directory information protections;
- 171 (3){(c)} complies with the sensitive materials requirements described in Section 53G-10-103;
172 (4){(d)} {~~unless an LEA obtains parental consent in accordance with Section 53G-10-402,~~} requires
that educational software may not display, recommend, algorithmically generate, or provide access
to any instructional or supplemental content that constitutes:
- 175 {(a) {~~human sexuality instruction;~~}
200 (i) pornographic or indecent material as that term is defined in Section 76-5c-208; or
176 (b){(ii)} sexual {~~education~~} exploitation or abuse;
177 {(c) {~~maturation instruction;~~}
178 {(d) {~~content relating to reproduction, contraception, sexual activity, or sexually transmitted diseases;~~
or-}
- 180 {(e) {~~sexual-health-related information;~~}
181 (5){(e)} prohibits addictive design features;
182 (6){(f)} prohibits a vendor from collecting, storing, or analyzing;

SB0267 compared with SB0267S02

- 183 (a){(i)} biometric identifiers, except for:
- 184 (i){(A)} voice recognition for speech-to-text accessibility features;or
- 185 {(ii)} {~~facial recognition for identity verification with parental consent; or~~};
- 186 (iii){(B)} other biometric data explicitly required for {~~educational accessibility~~} a student's IEP or
Section 504 accommodation plan; and
- 187 (b){(ii)} behavioral or emotional signals for purposes of:
- 188 (i){(A)} psychological profiling;
- 189 (ii){(B)} emotional manipulation;
- 190 (iii){(C)} commercial marketing or advertising; or
- 191 (iv){(D)} any purpose other than improving educational outcomes;
- 192 {(e)} {~~voice-prints or keystroke dynamics for a purpose other than:~~};
- 193 {(i)} {~~speech-enabled learning applications;~~};
- 194 {(ii)} {~~accessibility accommodations;~~};
- 195 {(iii)} {~~typing instruction or assessment; or~~};
- 196 {(iv)} {~~preventing academic dishonesty; and~~};
- 197 {(d)} {~~precise geolocation, except for:~~};
- 198 {(i)} {~~school bus tracking applications;~~};
- 199 {(ii)} {~~emergency safety features; or~~};
- 200 {(iii)} {~~field trip management with parental consent;~~};
- 201 (7){(g)} provides that any data collected under Subsection {(6)} (1)(f):
- 202 (a){(i)} is disclosed in the statewide digital privacy agreement;
- 203 (b){(ii)} is the minimum amount necessary for the educational purpose;
- 204 (c){(iii)} is not used for commercial purposes; and
- 205 (d){(iv)} is subject to strict security safeguards;
- 206 {(8)} {~~unless the software used in the classroom is integral to the subject matter of the course, prohibits~~
~~software from:~~};
- 207 {(a)} {~~using student data to train machine-learning models for commercial purposes unrelated to~~
~~improving educational outcomes for students;~~};
- 210 {(b)} {~~employing artificial intelligence systems that analyze a student's emotions, behavior, or attention~~
~~for purposes other than:~~};
- 212 {(i)} {~~providing personalized academic instruction, tutoring, or assessment;~~};

SB0267 compared with SB0267S02

- 213 {~~(ii) {identifying a student who may need additional academic support;}~~}
- 214 {~~(iii) {adapting educational content to a student's demonstrated learning needs; or}~~}
- 215 {~~(iv) {measuring academic progress and learning outcomes;}~~}
- 216 {~~(e) {generating or recommending content intended to influence a student's personal, political, or religious beliefs; or}~~}
- 218 {~~(d) {using persuasive design techniques, behavioral nudges, or psychological manipulation to maximize time-on-platform rather than learning outcomes;}~~}
- 220 (9){(h)} requires a vendor to:
- 221 (a){(i)} use encryption for data in transit and at rest;
- 222 {~~(b) {store and process all student data within the United States;}~~}
- 223 (c){(ii)} disclose ~~{all sub-processors and obtain approval before}~~ the use{:} of sub-processors; and
- 224 {~~(d) {prohibit background data collection when software is minimized or inactive; and}~~}
- 225 (e){(iii)} disclose to the contracting entity all data elements collected, third-party recipients, embedded libraries and analytics tools, device-level permissions, and artificial intelligence components and functions;
- 228 (10){(i)} prohibits educational software from accessing a device's camera and microphone unless:
- 229 (a){(i)} necessary for an educational function; and
- 230 (b){(ii)} disclosed in the digital privacy agreement;
- 231 (11){(j)} prohibits a vendor from conditioning access, features, pricing, or support on a:
- 232 (a){(i)} usage quota; or
- 233 (b){(ii)} screen-time expectation; ~~and~~}
- 234 (12){(k)} includes a termination-for-cause provision that:
- 235 (a){(i)} requires the vendor to cure any violation of the digital privacy agreement within a timeline the state board establishes;
- 237 (b){(ii)} authorizes the contracting entity to terminate the contract if the vendor fails to cure the violation of the digital privacy agreement required under Subsection ~~{(11)(a)}~~ (1)(k)(i);
- 239 (c){(iii)} provides that the termination described in this Subsection ~~{(12)}~~ (1)(k) may occur without penalty, early-termination fee, or additional obligation to the contracting entity;
- 241 (d){(iv)} requires the vendor to acknowledge that termination under this Subsection ~~{(12)}~~ (1)(k) does not constitute a breach by the contracting entity; and

243

SB0267 compared with SB0267S02

(e){(v)} when a vendor fails to cure as required under Subsection {(12)(a)} (1)(k)(i), authorizes the state board to direct the contracting entity to terminate the contract or terminate the contracting entity's participation in the contract on the contracting entity's behalf{-} ; and

246 (1) prohibits educational software that a vendor designs for peer-to-peer communication unless the educational software includes an administrative control that enables an administrator to turn peer-to-peer communication on or off.

249 (2) Notwithstanding the requirements of Subsection (1) the state board may allow a contracting entity to modify the statewide data privacy agreement if the state board determines the modification to be necessary for a contract with a specific vendor.

252 (3)

(a) A contracting entity may use administrative software without executing the statewide digital privacy agreement.

254 (b) Before a contracting entity uses administrative software, the contracting entity shall execute a digital privacy agreement that includes the requirements described in Subsection (1)(b).

257 (4) This part does not apply to a telecommunications carrier or internet service provider, or to any affiliate of the telecommunication carrier or internet service provider, when acting solely as a passive conduit for the transmission, routing, or provision of internet connectivity or network access for software or digital services a student uses, including:

261 (a) the transmission or routing of data packets;

262 (b) the provision of wireless or broadband connectivity;

263 (c) network management, quality-of-service, cybersecurity, or fraud-prevention functions; or

265 (d) the provision of device-level operating systems or firmware updates that are not designed to collect, analyze, or monetize student data.

267 Section 3. Section 3 is enacted to read:

268 **53G-7-1403. Vendor -- Duties.**

248 (1)

(a) Before the vendor allows {an individual} a contracting entity to install, assign, {recommend,} or otherwise make the educational software available for student use, the vendor shall:

250 (i) execute the statewide digital privacy agreement; and

272

SB0267 compared with SB0267S02

(ii) subject to Section 53G-7-1407, verify that the educational software is academically effective through self-verification or independent verification, in accordance with the process the state board creates in Section 53G-7-1405.

275 (b) A vendor that self-certifies for academic effectiveness shall:

251 ~~(ii){(i) {procure an independent verification of } submit to the {software to demonstrate } state board a written certification that the {vendor's } educational software is academically effective{-} ; and~~

253 ~~{(b) {Notwithstanding Subsection (1)(a)(ii), a vendor may make software available for use to a contracting entity on a provisional basis for up to 24 months from the initial deployment of the software if:-} }~~

256 ~~{(i) {the vendor submits a verification plan to the state board within 90 days of initial use, including:-} }~~

258 ~~{(A) {a proposed methodology for demonstrating academic effectiveness;-} }~~

259 ~~{(B) {a timeline for completion of independent verification; and}-} }~~

260 ~~{(C) {interim measures to assess educational value; and}-} }~~

261 ~~(ii) {the vendor demonstrates to } comply with the rules and timelines the state board {that the software:-} establishes under Section 53G-7-1405.~~

262 ~~{(A) {aligns with state core education standards;-} }~~

263 ~~{(B) {has research-supported pedagogical design; or}-} }~~

264 ~~{(C) {has been successfully used in other comparable educational settings;-} }~~

265 ~~{(e) {During the provisional period described in Subsection (1)(b), the contracting entity and vendor shall collect data necessary for academic effectiveness verification.-} }~~

267 (2) A vendor shall:

268 ~~{(a) {include the following in the process of obtaining the independent verification described in Subsection (1)(a):-} }~~

270 ~~{(i) {a description of the evaluator's research or evaluation methods;-} }~~

271 ~~{(ii) {identification of the student populations, grade levels, or instructional contexts under evaluation;-} }~~

273 ~~{(iii) {evidence that the vendor did not produce, fund, or influence the results;-} }~~

274 ~~{(iv) {disclosure of any limitations in the evidence or methodology; and}-} }~~

275 ~~{(v) {a determination of whether the software provides educational value sufficient to justify classroom use;-} }~~

SB0267 compared with SB0267S02

- 277 (b){(a)} provide the state board access to all records, documents, and data necessary to complete the
audits described in Section 53G-7-1405; and
- 279 (c){(b)} execute the statewide digital privacy agreement before providing educational software or
digital services to a contracting entity.
- 281 (3) A vendor may appeal a finding of noncompliance, issued under Section 53G-7-1405, through the
administrative process the state board establishes.
- 283 ~~{(4) {A vendor may not alter, supplement, replace, or modify the statewide digital privacy agreement.}}~~
}
- 285 (5){(4)} A vendor-proposed privacy agreement, end-user license agreement, click-through terms, terms
of service, or substitute contract is void and unenforceable with respect to student data or student
use.
- 290 (5) A vendor may not:
- 291 (a) alter, supplement, replace, or modify the statewide digital privacy agreement; or
- 288 (6){(b)} ~~{A vendor may not}~~ request or require that a parent or contracting entity:
- 289 (a){(i)} waive any right under this part;
- 290 (b){(ii)} agree to arbitration that limits this part; or
- 291 (c){(iii)} accept liability limitations inconsistent with this part.
- 296 Section 4. Section 4 is enacted to read:
- 297 **53G-7-1404. Contracting Entity -- Duties.**
- 294 (1) A contracting entity shall:
- 295 (a) execute the statewide digital privacy agreement for any educational software the contracting entity
adopts;
- 297 (b) unless the entity is contracting for {a} an educational software that the state board has previously
approved and listed on the list described in Subsection {53G-7-1405(1)(a)(v)} 53G-7-1405(1)(a)
(iv), obtain documentation of a vendor's {independent} verificationof academic effectiveness,
{described} in {Subsection 53G-7-1403(1)(b), demonstrating that the software is academically
effective before the contracting entity makes} accordance with the timelines and rules the state
board establishes under Section 53G-7-1405, before continuing use of the educational software
{available} for an individual to:
- 302 (i) install;
- 303 (ii) assign;or

SB0267 compared with SB0267S02

- 304 {~~(iii)~~ {~~recommend; or~~}}
- 305 (iv){~~(iii)~~} make available for student use;
- 306 (c) submit to the state board for listing:
- 307 (i) the executed statewide digital privacy agreement required under Subsection (1)(a); and
- 309 (ii) if necessary under Subsection (1)(b), the verification documentation described in Subsection (1)(b);
and
- 311 (d) provide the state board access to all records, documents, and data necessary to complete the audits
described in Section 53G-7-1405.
- 313 {~~(2)~~ {~~A contracting entity may not alter, supplement, replace, or modify the statewide digital privacy
agreement.~~}}
- 315 (3){~~(2)~~} A contracting entity may appeal a finding of noncompliance the state board issues under
Section 53G-7-1405 through the administrative process the state board establishes.
- 317 (4){~~(3)~~}
- (a) A contracting entity that is not the state board may request a modification to the statewide data
privacy agreement in accordance with Subsection 53G-7-1402(2).
- 321 (b) Except as provided in Subsection (4)(a), a contracting entity may not alter, supplement, replace, or
modify the statewide digital privacy agreement.
- 323 (4)
- (a) A contracting entity shall ensure that a digital privacy agreement between a vendor and a contracting
entity executed before {~~July~~} January 1, {~~2026~~} 2028, complies with the requirements of this
section before July 1, 2029.
- 320 (b) Between {~~July~~} January 1, {~~2026~~} 2028, and July 1, 2029, a contracting entity may continue to
use an existing digital privacy agreement if the contracting entity actively works toward compliance
with the statewide digital privacy agreement.
- 329 Section 5. Section 5 is enacted to read:
- 330 **53G-7-1405. State board and local education agencies -- Compliance -- Duties.**
- 325 (1)
- (a) The state board shall:
- 326 (i) ensure that educational software is not available for use in student instruction without {~~an
independent evaluator~~} verifying the software for academic effectiveness;
- 328

SB0267 compared with SB0267S02

- (ii) maintain a public list of independent evaluators that ~~{meet the standards described in Subsection 53G-7-1403(2)(a)}~~ a vendor may use to verify educational software as academically effective;
- 330 ~~{(iii) {create and maintain a statewide master list of software that students use in public schools;}}~~
- 332 (iv)~~{(iii)}~~ place educational software on the master list described in Subsection ~~{(1)(a)(iii)}~~ (1)(a)(iv) when a contracting entity, in accordance with Section 53G-7-1404:
- 334 (A) executes a statewide digital privacy agreement; and
- 335 (B) ~~{obtains verification}~~ verifies that the educational software is academically effective; ~~{and}~~
- 336 (v)~~{(iv)}~~ create and maintain a master list of all educational software the state board approves for student use under this section~~{:}~~ ; and
- 342 (v) before July 1, 2028, create a process that allows a vendor to demonstrate academic effectiveness through:
- 344 (A) vendor self-verification; or
- 345 (B) third-party verification.
- 346 (b) The state board may consult software vendors for technical input regarding functionality or implementation of the requirements of this section.
- 338 (b)~~{(c)}~~ ~~{A}~~ An educational software's exclusion from the master list does not prevent a contracting entity from using the software if the software meets the requirements of Section 53G-7-1404.
- 340 (c)~~{(d)}~~ ~~{A}~~ An educational software's inclusion on the master list described in Subsection (1)(a)(iii) does not constitute state board approval or endorsement.
- 342 (2)
- (a) The state board shall:
- 343 (i) monitor and enforce compliance with this section through periodic audits of:
- 344 (A) contracting entities; and
- 345 (B) vendors;
- 346 (ii) beginning July 1, 2029, audit each LEA, at least once every three years, to confirm that, for every educational software product students use that is not on the state board approved list described in Subsection (1)(a)(v), the LEA has:
- 349 (A) executed the statewide digital privacy agreement; and
- 350 (B) obtained the verification documentation;
- 351 (iii) in performing the audits required under Subsection (2)(a)(i), review vendor compliance with:

SB0267 compared with SB0267S02

- 353 (A) the requirements of this part; and
- 354 (B) Title 53E, Chapter 9, Student Privacy and Data Protection; and
- 355 (iv) issue a written compliance report, following each audit required under this Subsection (2)(a),
identifying:
- 357 (A) findings of compliance and noncompliance;
- 358 (B) required corrective actions; and
- 359 (C) applicable timelines for remediation.
- 360 (b) The state board may publish audit findings under Subsection (2)(a) to:
- 361 (i) promote transparency; and
- 362 (ii) make the public aware of compliant and noncompliant practices.
- 363 (3) If the state board finds an LEA to be out of compliance with the requirements of Section
53G-7-1404, the LEA shall:
- 365 (a) discontinue use of the noncompliant educational software;
- 366 (b) remedy the source of the noncompliance; and
- 367 (c) implement a corrective-action plan to prevent future violations.
- 368 (4) The state board shall provide:
- 369 (a) technical guidance and transition support to contracting entities and vendors regarding the transition
to the statewide digital privacy agreement and academic effectiveness requirements; and
- 372 (b) implementation timelines and instructions necessary for contracting entities to achieve compliance.
- 374 (5) The state board may prioritize technical guidance and transition support for:
- 375 (a) vendors executing digital privacy agreements with multiple contracting entities;
- 376 (b) statewide or consortium contracts; or
- 377 (c) software with known privacy, safety, or effectiveness concerns.
- 378 (6) An LEA may not use software other than {instructional} educational software in a public school for
instruction of a student.
- 380 (7) Before an LEA enters into a digital privacy agreement with a vendorfor educational software, the
LEA shall ensure that the digital privacy agreement meets each of the requirements of the statewide
digital privacy agreement the state board creates under Section 53G-7-1402.
- 383 (8) An LEA shall:
- 384 (a) provide a parent, annually, with a list of all {instructional} educational software products:
- 385 (i) for which the vendor has executed a statewide digital privacy agreement;

SB0267 compared with SB0267S02

- 386 (ii) for which a vendor has completed the {independent} verification of academic effectiveness
387 required under Section 53G-7-1403; and
- 388 (iii) that the LEA may assign, require, recommend, or otherwise made available for student use during
389 the upcoming school year;
- 390 (b) ensure that the list described in Subsection (8)(a) includes, at minimum:
- 391 (i) the product name and vendor;
- 392 (ii) the educational software's primary instructional purpose;
- 393 (iii) a link to the educational software's statewide digital privacy agreement; and
- 394 (iv) except as provided in Section 53G-7-1407, a link to the academic effectiveness verification a
395 vendor is required to produce under Section 53G-7-1403;
- 396 (c) publish the list described in Subsection (8)(a) on the LEA's public website;
- 397 (d) update the list described in Subsection (8)(a) within 10 business days of any addition or removal of
398 {a} an educational software product;
- 399 (e) for any {instructional} educational software added during the course of the school year:
- 400 (i) provide written notice to parents within 10 school days of the products approval;
- 401 (ii) include links to the product's statewide digital privacy agreement and academic-effectiveness
402 verification summary; and
- 403 (iii) provide {this} the notice, described in Subsection (8)(e)(i), before assigning the educational
404 software or making it available for student use;
- 405 (f) provide parents with written notice of any significant software update or change in data-collection or
406 data-sharing practices that:
- 407 (i) may affect compliance with the statewide digital privacy agreement; or
- 408 (ii) may trigger new consent requirements under state or federal law; and
- 409 (g) maintain a publicly accessible archive of {instructional} educational software that students
410 previously used, including:
- 411 (i) the software name and vendor; and
- 412 (ii) the dates during which the product was in active use.
- 413 (9) In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, the state board shall
414 make rules to implement the requirements of this part, including rules to:
- 415 (a) create a statewide digital privacy agreement;
- 416
- 417

SB0267 compared with SB0267S02

- (b) create an administrative process for a parent to submit a complaint in accordance with Section 53G-7-1406;
- 419 (c) create a process for vendors and contracting entities to appeal a finding of noncompliance;
- 421 (d) before January 1, 2028, create a process for ensuring all educational software is academically effective{;}, including:
- 435 (i) classifying software based on whether the software is:
- 436 (A) student-facing and if the student uses the software directly for instruction, practice, assessment, feedback, communication, collaboration, accessibility, or other learning-related interaction; or
- 439 (B) used solely for administrative or technical infrastructure functions;
- 440 (ii) requiring evaluation of educational software within each classification and establishing classification-specific methodologies or evidentiary standards for determining whether educational software provides, enables, or supports:
- 443 (A) active learning;
- 444 (B) skill development; or
- 445 (C) academic progress; and
- 446 (iii) creating the verification process described in Subsection (1)(a)(v);
- 422 (e) create standards and a process for approving and listing the educational software described in Subsection (1)(a)(v);
- 424 (f) create and maintain the master list described in Subsection (1)(a)(iii);
- 425 (g) conduct the audits required under Subsection (2)(a); and
- 426 (h) create a process for receiving and responding to complaints a parent submits under Section 53G-7-1406.
- 453 Section 6. Section 6 is enacted to read:
- 454 **53G-7-1406. Complaints -- Enforcement.**
- 430 (1)
- (a) A parent may submit a written complaint to the state board alleging:
- 431 (i) a contracting entity {using} using educational software without executing a statewide digital privacy agreement;
- 433 (ii) a contracting entity using educational software without being verified as academically effective; or
- 435 (iii) a vendor's violation of the statewide digital privacy agreement.

SB0267 compared with SB0267S02

436 (b) Upon receiving a complaint described in Subsection (1)(a), the state board shall consult with the
437 Office of the Attorney General to:

438 (i) review the complaint;

439 (ii) determine if a violation has occurred;

440 (iii) notify the parent of the determination; and

441 (iv) take appropriate enforcement action under this part if noncompliance is found.

442 (2) A court shall award the Office of the Attorney General reasonable attorney fees, court costs, and
investigative expenses incurred in an action under this part.

469 Section 7. Section 7 is enacted to read:

470 **53G-7-1407. Provisional software.**

471 (1) Notwithstanding Subsection 53G-7-1403(1)(a)(ii) and before July 1, 2028, a vendor may make
educational software available for use to a contracting entity on a provisional basis for up to 24
months from the initial deployment of the software if:

474 (a) the vendor submits a verification plan to the contracting entity before the educational software is
made available for student use, including:

476 (i) a proposed methodology for demonstrating academic effectiveness;

477 (ii) a timeline for completion of verification of academic effectiveness; and

478 (iii) interim measures to assess active learning, skill development, or academic progress in the intended
subject area; and

480 (b) the vendor demonstrates to the contracting entity that the educational software:

481 (i) aligns with state core education standards; and

482 (ii) meets an educational purpose.

483 (2) A student may not use educational software made available under Subsection (1)(a) without consent
from the student's parent.

485 (3) A contracting entity shall notify a student's parent of:

486 (a) the implementation of educational software on a provisional basis in accordance with Subsection (1)
(a); and

488 (b) the consent required to use the educational software under Subsection (1)(b).

489 (4) During the provisional period described in Subsection (1)(a), the contracting entity and vendor
shall collect data necessary for academic effectiveness verification in accordance with the statewide
digital privacy agreement.

SB0267 compared with SB0267S02

492

Section 8. **Effective date.**

Effective Date.

This bill takes effect on July 1, 2026.

3-2-26 5:03 PM