

Kirk A. Cullimore proposes the following substitute bill:

**Software in Education Amendments**

2026 GENERAL SESSION

STATE OF UTAH

**Chief Sponsor: Kirk A. Cullimore**

House Sponsor:

---

---

**LONG TITLE**

**General Description:**

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

**Highlighted Provisions:**

This bill:

- defines terms;
- requires the State Board of Education to:
  - create a statewide digital privacy agreement;
  - ensure that all software used in a public school is executed under the statewide digital privacy agreement and academically effective;
  - create a master list for software used in public schools;
  - create a list of approved software;
  - independently verify software as academically effective;
  - enforce compliance with the requirements of this section through periodic audits;
  - create a process for a parent to submit a complaint; and
  - create rules to implement the requirements of this section;
- creates a certain exception;
- requires a local education agency (LEA), the Utah Education and Telehealth Network, and the State Board of Education to:
  - execute the statewide digital privacy agreement for all software contracts; and
  - verify certain software is academically effective;
- requires an LEA to notify parents of all software a public school uses during the school year;
- requires the state board to consult with the Office of the Attorney General; and
- requires a vendor to:



- 63           (v) other recognized evidence based learning strategies;  
64           (d) does not employ design features that primarily:  
65               (i) interfere with active learning; or  
66               (ii) undermine teacher instructional authority; and  
67           (e) produces positive academic outcomes when used as intended.  
68   (2) "Active learning" means instruction that requires a student to engage in cognitive  
69       processes including analyzing, reasoning, practicing, or creating to understand or apply  
70       knowledge or skills.  
71   (3)(a) "Addictive design feature" means a feature or component of a digital or online  
72       product that encourages or increases a student's frequency, time spent, or engagement  
73       with the product.  
74       (b) "Addictive design feature" includes the following features:  
75           (i) infinite scroll;  
76           (ii) autoplay that continues beyond the educational task or lesson;  
77           (iii) points, badges, or other gamification rewards tied to time spent on the product  
78               rather than learning objectives or academic progress;  
79           (iv) persistent notifications prompting re-engagement when the product is not  
80               actively in use, unless:  
81                (A) a teacher initiates the notification; and  
82                (B) the notification is directly related to assigned schoolwork;  
83           (v) personalized recommendation systems designed to maximize time-on-platform  
84               rather than learning outcomes; or  
85           (vi) engagement metrics, streaks, or social comparison features designed to create  
86               fear of missing out or compulsive checking behavior.  
87       (c) "Addictive design feature" does not include a:  
88           (i) recommendation of next lessons or learning activities based on curriculum  
89               progression or mastery of prerequisites;  
90           (ii) notification about a teacher-assigned or course-required assignment, deadline, or  
91               teacher feedback; or  
92           (iii) feature that encourages active learning rather than passive consumption.  
93   (4) "Clickstream data" means data an LEA or third-party provider collects from a student's  
94       use of an online service, application, or device that records the student's navigation or  
95       sequence of actions.  
96   (5) "Contracting entity" means the following entities if that entity contracts with a vendor

97 for software:

98 (a) an LEA;

99 (b) the state board; or

100 (c) UETN.

101 (6) "Digital privacy agreement" means a contract between a contracting entity and a digital  
102 provider that:

103 (a) ensures compliance with Title 53E, Chapter 9, Student Privacy and Data Protection;  
104 and

105 (b) governs access, use, protection, retention, and disclosure of student data.

106 (7)(a) "Educational purpose" means a purpose directly related to:

107 (i) student instruction;

108 (ii) assessment of a student; or

109 (iii) school operations necessary for instruction of a student.

110 (b) "Educational purpose" does not include:

111 (i) marketing;

112 (ii) advertising;

113 (iii) behavioral profiling; or

114 (iv) any other commercial purpose.

115 (8) "Independently verified" means software that an impartial third party, with no financial  
116 or contractual relationship with the vendor and with demonstrated expertise appropriate  
117 to the type of software, checks for:

118 (a) safety;

119 (b) effectiveness; and

120 (c) compliance with the requirements of this part.

121 (9) "Instructional software" means software that is safe, legal, and effective because the  
122 software is:

123 (a) part of a digital privacy agreement; and

124 (b) verified for academic effectiveness in accordance with the requirements of this  
125 section.

126 (10) "Internet service provider" means the same as that term is defined in Section 76-5c-401.

127 (11) "Passive consumption" means receiving information through viewing, listening, or  
128 browsing without requiring the student to engage in cognitive processing necessary to  
129 analyze, apply, or create knowledge or skills.

130 (12) "School-issued device" means any electronic hardware device an LEA provides to a

- 131 student for educational use.
- 132 (13)(a) "Software" means any application, web-based service, plug-in, or other  
133 code-based product, regardless of whether the application is free or for purchase, that:
- 134 (i) runs on or is accessible from a school-issued device or from a student-owned  
135 device that the student uses for the student's education; and
- 136 (ii) an LEA assigns, requires, recommends, installs, or otherwise makes available for  
137 student use in connection with classroom instruction.
- 138 (b) "Software" includes software an individual uses in connection with school-related  
139 purposes for:
- 140 (i) instruction;
- 141 (ii) assessment;
- 142 (iii) communication;
- 143 (iv) collaboration;
- 144 (v) enrichment; or
- 145 (vi) recreation.
- 146 (c) "Software" does not include physical, electronic hardware.
- 147 (14) "Statewide digital privacy agreement" means the digital privacy agreement the state  
148 board creates in accordance with Section 53G-7-1402.
- 149 (15)(a) "Student data" means the same as that term is defined in Section 53E-9-301.
- 150 (b) "Student data" includes a student's:
- 151 (i) personally identifiable information;
- 152 (ii) metadata, device identifiers, and clickstream data;
- 153 (iii) behavioral, engagement, or usage data; and
- 154 (iv) information a software collects, generates, or infers in the course of student use.
- 155 (16) "Sub-processor" means a third-party vendor or service that a primary data processor  
156 engages to process personal data on the processor's behalf.
- 157 (17)(a) "Telecommunications carrier" means an entity that provides transmission,  
158 routing, or connectivity services for digital communications, including wireless,  
159 broadband, or data transport services, without modifying the content of  
160 communications.
- 161 (b) "Telecommunications carrier" includes an internet service provider.
- 162 (18) "Utah Education and Telehealth Network" or "UETN" means the same as that term is  
163 defined in Section 53H-4-213.1.
- 164 (19)(a) "Vendor" means an entity that provides software, digital tools, digital services, or

165 related technology to a contracting entity for student use, whether free or paid.

166 (b) "Vendor" does not include:

167 (i) a telecommunications carrier; or

168 (ii) an internet service provider.

169 (20) "Voice-print" means a digital representation of an individual's voice that a person  
 170 creates, derives, or uses to identify or authenticate the individual.

171 Section 2. Section **53G-7-1402** is enacted to read:

172 **53G-7-1402 . Statewide digital privacy agreement -- Exceptions.**

173 (1) The state board shall create a form statewide digital privacy agreement that:

174 (a) governs student use of software and digital services in public schools;

175 (b) complies with the requirements of Title 53E, Chapter 9, Student Privacy and Data  
 176 Protection, including:

177 (i) data minimization;

178 (ii) prohibitions on advertising or promotional content directed at a student, including:

179 (A) advertising products or services to a student while the student is using  
 180 software of instructional material;

181 (B) allowing a third-party to advertise a product or a service to a student; and

182 (C) the inclusion of advertising or promotional content within software of  
 183 instructional material accessible to a student;

184 (iii) limits on secondary data use;

185 (iv) security safeguards;

186 (v) breach notifications;

187 (vi) data retention and deletion requirements; and

188 (vii) directory information protections;

189 (c) complies with the sensitive materials requirements described in Section 53G-10-103;

190 (d) unless an LEA obtains parental consent in accordance with Section 53G-10-402,  
 191 requires that software may not display, recommend, algorithmically generate, or  
 192 provide access to any instructional or supplemental content that constitutes:

193 (i) human sexuality instruction;

194 (ii) sexual education;

195 (iii) maturation instruction;

196 (iv) content relating to reproduction, contraception, sexual activity, or sexually  
 197 transmitted diseases; or

198 (v) sexual-health-related information;

- 199 (e) prohibits addictive design features;
- 200 (f) prohibits a vendor from collecting, storing, or analyzing:
- 201 (i) biometric identifiers, except for:
- 202 (A) voice recognition for speech-to-text accessibility features; or
- 203 (B) other biometric data explicitly required for a student's IEP or Section 504
- 204 accommodation plan; and
- 205 (ii) behavioral or emotional signals for purposes of:
- 206 (A) psychological profiling;
- 207 (B) emotional manipulation;
- 208 (C) commercial marketing or advertising; or
- 209 (D) any purpose other than improving educational outcomes;
- 210 (g) provides that any data collected under Subsection (1)(f):
- 211 (i) is disclosed in the statewide digital privacy agreement;
- 212 (ii) is the minimum amount necessary for the educational purpose;
- 213 (iii) is not used for commercial purposes; and
- 214 (iv) is subject to strict security safeguards;
- 215 (h) requires a vendor to:
- 216 (i) use encryption for data in transit and at rest;
- 217 (ii) store and process all student data within the United States;
- 218 (iii) disclose all sub-processors and obtain approval before use;
- 219 (iv) prohibit background data collection when software is minimized or inactive; and
- 220 (v) disclose to the contracting entity all data elements collected, third-party
- 221 recipients, embedded libraries and analytics tools, device-level permissions, and
- 222 artificial intelligence components and functions;
- 223 (i) prohibits software from accessing a device's camera and microphone unless:
- 224 (i) necessary for an educational function; and
- 225 (ii) disclosed in the digital privacy agreement;
- 226 (j) prohibits a vendor from conditioning access, features, pricing, or support on a:
- 227 (i) usage quota; or
- 228 (ii) screen-time expectation; and
- 229 (k) includes a termination-for-cause provision that:
- 230 (i) requires the vendor to cure any violation of the digital privacy agreement within a
- 231 timeline the state board establishes;
- 232 (ii) authorizes the contracting entity to terminate the contract if the vendor fails to

233 cure the violation of the digital privacy agreement required under Subsection  
 234 (1)(k)(i);  
 235 (iii) provides that the termination described in this Subsection (1)(k) may occur  
 236 without penalty, early-termination fee, or additional obligation to the contracting  
 237 entity;  
 238 (iv) requires the vendor to acknowledge that termination under this Subsection (1)(k)  
 239 does not constitute a breach by the contracting entity; and  
 240 (v) when a vendor fails to cure as required under Subsection (1)(k)(i), authorizes the  
 241 state board to direct the contracting entity to terminate the contract or terminate  
 242 the contracting entity's participation in the contract on the contracting entity's  
 243 behalf.

244 (2) This part does not apply to a telecommunications carrier or internet service provider, or  
 245 to any affiliate of the telecommunication carrier or internet service provider, when acting  
 246 solely as a passive conduit for the transmission, routing, or provision of internet  
 247 connectivity or network access for software or digital services a student uses, including:  
 248 (a) the transmission or routing of data packets;  
 249 (b) the provision of wireless or broadband connectivity;  
 250 (c) network management, quality-of-service, cybersecurity, or fraud-prevention  
 251 functions; or  
 252 (d) the provision of device-level operating systems or firmware updates that are not  
 253 designed to collect, analyze, or monetize student data.

254 Section 3. Section **53G-7-1403** is enacted to read:

255 **53G-7-1403 . Vendor -- Duties.**

256 (1)(a) Before the vendor allows an individual to install, assign, recommend, or otherwise  
 257 make the software available for student use, the vendor shall:  
 258 (i) execute the statewide digital privacy agreement; and  
 259 (ii) procure an independent verification of the software to demonstrate that the  
 260 vendor's software is academically effective.  
 261 (b) Notwithstanding Subsection (1)(a)(ii), a vendor may make software available for use  
 262 to a contracting entity on a provisional basis for up to 24 months from the initial  
 263 deployment of the software if:  
 264 (i) the vendor submits a verification plan to the state board within 90 days of initial  
 265 use, including:  
 266 (A) a proposed methodology for demonstrating academic effectiveness;

- 267 (B) a timeline for completion of independent verification; and  
268 (C) interim measures to assess educational value; and  
269 (ii) the vendor demonstrates to the state board that the software:  
270 (A) aligns with state core education standards;  
271 (B) has research-supported pedagogical design; or  
272 (C) has been successfully used in other comparable educational settings.  
273 (c) A student may not use software made available under Subsection (1)(b) without  
274 consent from the student's parent.  
275 (d) A contracting entity shall notify a student's parent of:  
276 (i) the implementation of software on a provisional basis in accordance with  
277 Subsection (1)(b); and  
278 (ii) the consent required to use the software under Subsection (1)(c).  
279 (e) During the provisional period described in Subsection (1)(b), the contracting entity  
280 and vendor shall collect data necessary for academic effectiveness verification.  
281 (2) A vendor shall:  
282 (a) include the following in the process of obtaining the independent verification  
283 described in Subsection (1)(a):  
284 (i) a description of the evaluator's research or evaluation methods;  
285 (ii) identification of the student populations, grade levels, or instructional contexts  
286 under evaluation;  
287 (iii) evidence that the vendor did not produce, fund, or influence the results;  
288 (iv) disclosure of any limitations in the evidence or methodology; and  
289 (v) a determination of whether the software provides educational value sufficient to  
290 justify classroom use;  
291 (b) provide the state board access to all records, documents, and data necessary to  
292 complete the audits described in Section 53G-7-1405; and  
293 (c) execute the statewide digital privacy agreement before providing software or digital  
294 services to a contracting entity.  
295 (3) A vendor may appeal a finding of noncompliance, issued under Section 53G-7-1405,  
296 through the administrative process the state board establishes.  
297 (4) A vendor may not alter, supplement, replace, or modify the statewide digital privacy  
298 agreement.  
299 (5) A vendor-proposed privacy agreement, end-user license agreement, click-through terms,  
300 terms of service, or substitute contract is void and unenforceable with respect to student

301 data or student use.

302 (6) A vendor may not request or require that a parent or contracting entity:

303 (a) waive any right under this part;

304 (b) agree to arbitration that limits this part; or

305 (c) accept liability limitations inconsistent with this part.

306 Section 4. Section **53G-7-1404** is enacted to read:

307 **53G-7-1404 . Contracting Entity -- Duties.**

308 (1) A contracting entity shall:

309 (a) execute the statewide digital privacy agreement for any software the contracting  
310 entity adopts;

311 (b) unless the entity is contracting for a software that the state board has previously  
312 approved and listed on the list described in Subsection 53G-7-1405(1)(a)(v), obtain  
313 documentation of a vendor's independent verification, described in Subsection  
314 53G-7-1403(1)(b), demonstrating that the software is academically effective before  
315 the contracting entity makes the software available for an individual to:

316 (i) install;

317 (ii) assign;

318 (iii) recommend; or

319 (iv) make available for student use;

320 (c) submit to the state board for listing:

321 (i) the executed statewide digital privacy agreement required under Subsection (1)(a);  
322 and

323 (ii) if necessary under Subsection (1)(b), the verification documentation described in  
324 Subsection (1)(b); and

325 (d) provide the state board access to all records, documents, and data necessary to  
326 complete the audits described in Section 53G-7-1405.

327 (2) A contracting entity may not alter, supplement, replace, or modify the statewide digital  
328 privacy agreement.

329 (3) A contracting entity may appeal a finding of noncompliance the state board issues under  
330 Section 53G-7-1405 through the administrative process the state board establishes.

331 (4)(a) A contracting entity shall ensure that a digital privacy agreement between a  
332 vendor and a contracting entity executed before July 1, 2026, complies with the  
333 requirements of this section before July 1, 2028.

334 (b) Between July 1, 2026, and July 1, 2028, a contracting entity may continue to use an

335 existing digital privacy agreement if the contracting entity actively works toward  
336 compliance with the statewide digital privacy agreement.

337 Section 5. Section **53G-7-1405** is enacted to read:

338 **53G-7-1405 . State board and local education agencies -- Compliance -- Duties.**

339 (1)(a) The state board shall:

340 (i) ensure that software is not available for use in student instruction without an  
341 independent evaluator verifying the software for academic effectiveness;

342 (ii) maintain a public list of independent evaluators that meet the standards described  
343 in Subsection 53G-7-1403(2)(a);

344 (iii) create and maintain a statewide master list of software that students use in public  
345 schools;

346 (iv) place software on the master list described in Subsection (1)(a)(iii) when a  
347 contracting entity, in accordance with Section 53G-7-1404:

348 (A) executes a statewide digital privacy agreement; and

349 (B) obtains verification that the software is academically effective; and

350 (v) create and maintain a list of all software the state board approves for student use  
351 under this section.

352 (b) A software's exclusion from the master list does not prevent a contracting entity from  
353 using the software if the software meets the requirements of Section 53G-7-1404.

354 (c) A software's inclusion on the master list described in Subsection (1)(a)(iii) does not  
355 constitute state board approval or endorsement.

356 (2)(a) The state board shall:

357 (i) monitor and enforce compliance with this section through periodic audits of:

358 (A) contracting entities; and

359 (B) vendors;

360 (ii) beginning July 1, 2028, audit each LEA, at least once every three years, to  
361 confirm that, for every software product students use that is not on the state board  
362 approved list described in Subsection (1)(a)(v), the LEA has:

363 (A) executed the statewide digital privacy agreement; and

364 (B) obtained the verification documentation;

365 (iii) in performing the audits required under Subsection (2)(a)(i), review vendor  
366 compliance with:

367 (A) the requirements of this part; and

368 (B) Title 53E, Chapter 9, Student Privacy and Data Protection; and

- 369            (iv) issue a written compliance report, following each audit required under this  
370            Subsection (2)(a), identifying:  
371            (A) findings of compliance and noncompliance;  
372            (B) required corrective actions; and  
373            (C) applicable timelines for remediation.  
374        (b) The state board may publish audit findings under Subsection (2)(a) to:  
375            (i) promote transparency; and  
376            (ii) make the public aware of compliant and noncompliant practices.  
377        (3) If the state board finds an LEA to be out of compliance with the requirements of Section  
378        53G-7-1404, the LEA shall:  
379            (a) discontinue use of the noncompliant software;  
380            (b) remedy the source of the noncompliance; and  
381            (c) implement a corrective-action plan to prevent future violations.  
382        (4) The state board shall provide:  
383            (a) technical guidance and transition support to contracting entities and vendors  
384            regarding the transition to the statewide digital privacy agreement and academic  
385            effectiveness requirements; and  
386            (b) implementation timelines and instructions necessary for contracting entities to  
387            achieve compliance.  
388        (5) The state board may prioritize technical guidance and transition support for:  
389            (a) vendors executing digital privacy agreements with multiple contracting entities;  
390            (b) statewide or consortium contracts; or  
391            (c) software with known privacy, safety, or effectiveness concerns.  
392        (6) An LEA may not use software other than instructional software in a public school for  
393        instruction of a student.  
394        (7) Before an LEA enters into a digital privacy agreement with a vendor, the LEA shall  
395        ensure that the digital privacy agreement meets each of the requirements of the statewide  
396        digital privacy agreement the state board creates under Section 53G-7-1402.  
397        (8) An LEA shall:  
398            (a) provide a parent, annually, with a list of all instructional software products:  
399            (i) for which the vendor has executed a statewide digital privacy agreement;  
400            (ii) for which a vendor has completed the independent verification of academic  
401            effectiveness required under Section 53G-7-1403; and  
402            (iii) that the LEA may assign, require, recommend, or otherwise made available for

- 403 student use during the upcoming school year;
- 404 (b) ensure that the list described in Subsection (8)(a) includes, at minimum:
- 405 (i) the product name and vendor;
- 406 (ii) the software's primary instructional purpose;
- 407 (iii) a link to the software's statewide digital privacy agreement; and
- 408 (iv) a link to the academic effectiveness verification a vendor is required to produce
- 409 under Section 53G-7-1403;
- 410 (c) publish the list described in Subsection (8)(a) on the LEA's public website;
- 411 (d) update the list described in Subsection (8)(a) within 10 business days of any addition
- 412 or removal of a software product;
- 413 (e) for any instructional software added during the course of the school year:
- 414 (i) provide written notice to parents within 10 school days of the products approval;
- 415 (ii) include links to the product's statewide digital privacy agreement and
- 416 academic-effectiveness verification summary; and
- 417 (iii) provide this notice before assigning the software or making it available for
- 418 student use;
- 419 (f) provide parents with written notice of any significant software update or change in
- 420 data-collection or data-sharing practices that:
- 421 (i) may affect compliance with the statewide digital privacy agreement; or
- 422 (ii) may trigger new consent requirements under state or federal law; and
- 423 (g) maintain a publicly accessible archive of instructional software that students
- 424 previously used, including:
- 425 (i) the software name and vendor; and
- 426 (ii) the dates during which the product was in active use.
- 427 (9) In accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, the
- 428 state board shall make rules to implement the requirements of this part, including rules
- 429 to:
- 430 (a) create a statewide digital privacy agreement;
- 431 (b) create an administrative process for a parent to submit a complaint in accordance
- 432 with Section 53G-7-1406;
- 433 (c) create a process for vendors and contracting entities to appeal a finding of
- 434 noncompliance;
- 435 (d) create a process for ensuring all software is academically effective;
- 436 (e) create standards and a process for approving and listing the software described in

- 437            Subsection (1)(a)(v);
- 438            (f) create and maintain the master list described in Subsection (1)(a)(iii);
- 439            (g) conduct the audits required under Subsection (2)(a); and
- 440            (h) create a process for receiving and responding to complaints a parent submits under
- 441            Section 53G-7-1406.

442            Section 6. Section **53G-7-1406** is enacted to read:

443            **53G-7-1406 . Complaints -- Enforcement.**

- 444            (1)(a) A parent may submit a written complaint to the state board alleging:
- 445                    (i) a contracting entity using software without executing a statewide digital privacy
- 446                    agreement;
- 447                    (ii) a contracting entity using software without being verified as academically
- 448                    effective; or
- 449                    (iii) a vendor's violation of the statewide digital privacy agreement.
- 450            (b) Upon receiving a complaint described in Subsection (1)(a), the state board shall
- 451            consult with the Office of the Attorney General to:
- 452                    (i) review the complaint;
- 453                    (ii) determine if a violation has occurred;
- 454                    (iii) notify the parent of the determination; and
- 455                    (iv) take appropriate enforcement action under this part if noncompliance is found.
- 456            (2) A court shall award the Office of the Attorney General reasonable attorney fees, court
- 457            costs, and investigative expenses incurred in an action under this part.

458            Section 7. **Effective Date.**

459            This bill takes effect on July 1, 2026.