

Ryan D. Wilcox proposes the following substitute bill:

**School Cybersecurity Amendments**

2026 GENERAL SESSION

STATE OF UTAH

**Chief Sponsor: Ryan D. Wilcox**

Senate Sponsor:

---

---

**LONG TITLE**

**General Description:**

This bill directs the State Board of Education to establish minimum cybersecurity standards for local education agencies.

**Highlighted Provisions:**

This bill:

- prohibits certain devices in schools;
- directs the Cybersecurity Commission to make rules establishing minimum cybersecurity standards for local education agencies (LEAs) aligned with industry recognized frameworks;
- establishes a phased implementation timeline for LEA compliance;
- requires coordination among the Utah Cyber Center, the State Board of Education, and the Utah Education and Telehealth Network;
- establishes reporting requirements for cybersecurity incidents;
- requires the State Board of Education to provide implementation support and resources;
- includes a coordination clause to incorporate changes made to Section 53G-7-227 with changes made to that section in S.B. 69, School Device Revisions; and
- makes conforming changes.

**Money Appropriated in this Bill:**

None

**Other Special Clauses:**

This bill provides a coordination clause.

**Utah Code Sections Affected:**

AMENDS:

**53G-7-227 (Effective 05/06/26)**, as last amended by Laws of Utah 2025, First Special Session, Chapter 9

29 **63C-27-201 (Effective 05/06/26) (Repealed 07/01/32)**, as enacted by Laws of Utah 2022,  
 30 Chapter 153

31 **63C-27-202 (Effective 05/06/26) (Repealed 07/01/32)**, as enacted by Laws of Utah 2022,  
 32 Chapter 153

33 ENACTS:

34 **53G-8-901 (Effective 05/06/26)**, Utah Code Annotated 1953

35 **53G-8-902 (Effective 05/06/26)**, Utah Code Annotated 1953

36 **53G-8-903 (Effective 05/06/26)**, Utah Code Annotated 1953

37 **Utah Code Sections affected by Coordination Clause:**

38 **53G-7-227 (05/06/26)**, as last amended by Laws of Utah 2025, First Special Session,  
 39 Chapter 9

---

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

42 *The following section is affected by a coordination clause at the end of this bill.*

43 Section 1. Section **53G-7-227** is amended to read:

44 **53G-7-227 (Effective 05/06/26). Device prohibition.**

45 (1) As used in this section:

46 (a)(i) "AI glasses" means wearable eyewear, whether prescription or  
 47 non-prescription, that:

48 (A) incorporates one or more sensors, including cameras, microphones,  
 49 accelerometers, gyroscopes, or biometric sensors;

50 (B) uses artificial intelligence, machine learning algorithms, or neural networks to  
 51 process, analyze, or interpret data captured by the sensors in real-time or near  
 52 real-time;

53 (C) provides information, overlays, translations, identification, or other augmented  
 54 content to the wearer through visual displays, audio output, or haptic feedback;  
 55 and

56 (D) may transmit, store, or share data to external devices, networks, or  
 57 cloud-based services.

58 (ii) "AI glasses" does not include:

59 (A) prescription eyeglasses or sunglasses without electronic components;

60 (B) wearable devices used solely for reading glasses or vision correction without  
 61 data collection or processing capabilities;

62 (C) protective eyewear that contains only passive sensors without artificial

63 intelligence processing capabilities; or  
 64 (D) virtual reality headsets designed primarily for immersive gaming or  
 65 entertainment that are not suitable for continuous wear in public settings.

66 [(a)] (b) "Cellphone" means a handheld, portable electronic device that is designed to be  
 67 operated using one or both hands and is capable of transmitting and receiving voice,  
 68 data, or text communication by means of:

- 69 (i) a cellular network;
- 70 (ii) a satellite network; or
- 71 (iii) any other wireless technology.

72 [(b)] (c) "Cellphone" includes:

- 73 (i) a smartphone;
- 74 (ii) a feature phone;
- 75 (iii) a mobile phone;
- 76 (iv) a satellite phone; or
- 77 (v) a personal digital assistant that incorporates capabilities similar to a smartphone,  
 78 feature phone, mobile phone, or satellite phone.

79 [(c)] (d) "Classroom hours" means:

80 (i) time during which a student receives scheduled, teacher-supervised instruction  
 81 that occurs:

- 82 (A) in a physical or virtual classroom setting;
- 83 (B) during regular school operating hours; and
- 84 (C) as part of an approved educational curriculum.

85 (ii) "Classroom hours" does not include:

- 86 (A) lunch periods;
- 87 (B) recess;
- 88 (C) transit time between classes;
- 89 (D) study halls unless directly supervised by a qualified instructor;
- 90 (E) after-school activities unless part of an approved extended learning program; or
- 91 (F) independent study time occurring outside scheduled instruction.

92 [(d)] (e)(i) "Emerging technology" means any other device that has or will be able to  
 93 act in place of or as an extension of an individual's cellphone.

94 (ii) "Emerging technology" does not include school provided or required devices.

95 [(e)] (f) "Smart watch" means a wearable computing device that closely resembles a  
 96 wristwatch or other time-keeping device with the capacity to act in place of or as an

97 extension of an individual's cellphone.

98 [(f)] (g) "Smart watch" does not include a wearable device that can only:

99 (i) tell time;

100 (ii) monitor an individual's health informatics;

101 (iii) receive and display notifications or information without the capability to  
102 respond; or

103 (iv) track the individual's physical location.

104 (2)(a) An LEA:

105 (i) shall establish a policy that allows a student to use a cellphone, smart watch, AI  
106 glasses, or emerging technology:

107 (A) to respond to an imminent threat to the health or safety of an individual;

108 (B) to respond to a school-wide emergency;

109 (C) to use the SafeUT Crisis Line described in Section 53H-4-210;

110 (D) for a student's IEP or Section 504 accommodation plan; or

111 (E) to address a medical necessity; and

112 (ii) may establish a policy that provides for other circumstances when a student may  
113 use a cellphone, smart watch, AI glasses, or emerging technology.

114 (b) An LEA may establish policies that:

115 (i) extend restrictions on student use of cellphones, smart watches, or emerging  
116 technologies to non-classroom hours during the school day, including:

117 (A) lunch periods;

118 (B) transition times between classes; and

119 (C) other school-supervised activities; and

120 (ii) impose additional limitations on the use of cellphones, smart watches, or  
121 emerging technologies beyond those required by this section.

122 (3) Except as provided in Subsection (2), a student may not use a cellphone, smart watch,  
123 AI glasses, or emerging technology at a school during classroom hours.

124 (4) The state board may create one or more model policies regarding when a student may  
125 use a student's cellphone, smart watch, AI glasses, or emerging technology in a school  
126 during classroom hours consistent with this section.

127 Section 2. Section **53G-8-901** is enacted to read:

128 **Part 9. LEA Cybersecurity Standards**

129 **53G-8-901 (Effective 05/06/26). General provisions -- Definitions.**

130 As used in this part:

- 131 (1) "Cyber Center" means the Utah Cyber Center created in Section 63A-16-1102.  
 132 (2) "Data breach" means the same as that term is defined in Section 63A-16-1101.  
 133 (3) "UETN" means the Utah Education and Telehealth Network created in Section  
 134 53H-4-213.4.

135 Section 3. Section **53G-8-902** is enacted to read:

136 **53G-8-902 (Effective 05/06/26). LEA compliance with cybersecurity standards --**  
 137 **Coordination.**

- 138 (1) An LEA shall comply with the minimum cybersecurity standards established by the  
 139 Cybersecurity Commission created in Section 63C-27-201 in rule made in accordance  
 140 with Subsection 63C-27-202(9).  
 141 (2) An LEA shall comply with the minimum cybersecurity standards according to the  
 142 phased implementation timeline established in rule under Subsection 63C-27-202(9).  
 143 (3) UETN, in consultation with the Cyber Center and the state board, shall:  
 144 (a) develop implementation guidelines and technical resources to assist LEAs in  
 145 meeting the minimum cybersecurity standards;  
 146 (b) provide technical assistance and support to LEAs; and  
 147 (c) coordinate the provision of cybersecurity services and resources to LEAs.  
 148 (4)(a) The Cyber Center, the state board, and UETN shall coordinate services to LEAs  
 149 to:  
 150 (i) avoid duplication of efforts;  
 151 (ii) maximize the effectiveness of cybersecurity resources;  
 152 (iii) ensure LEAs receive consistent guidance and support; and  
 153 (iv) facilitate information sharing regarding cybersecurity threats and best practices.  
 154 (b) The coordination required under Subsection (4)(a) shall include:  
 155 (i) regular meetings among the entities to discuss LEA cybersecurity needs and  
 156 initiatives;  
 157 (ii) joint development of training materials and resources;  
 158 (iii) coordinated response to cybersecurity incidents affecting LEAs; and  
 159 (iv) alignment of cybersecurity standards and network infrastructure requirements.

160 Section 4. Section **53G-8-903** is enacted to read:

161 **53G-8-903 (Effective 05/06/26). Data breach reporting -- Coordination with**  
 162 **Utah Cyber Center.**

- 163 (1) An LEA shall report a data breach to the Cyber Center:  
 164 (a) in accordance with Section 63A-19-405; and

- 165 (b) consistent with standards and procedures established in rule under Subsection  
166 63C-27-202(9).
- 167 (2) In addition to the requirements in Section 63A-19-405, an LEA shall:
- 168 (a) notify the state board within 24 hours of discovering the data breach;  
169 (b) coordinate with UETN if the data breach involves network infrastructure or services  
170 provided by UETN; and  
171 (c) cooperate with the Cyber Center's investigation and response efforts.
- 172 (3) The Cyber Center shall provide assistance to an LEA in responding to a data breach in  
173 the same manner the Cyber Center provides assistance to a governmental entity as  
174 described in Title 63A, Chapter 16, Part 11, Utah Cyber Center.
- 175 (4) An LEA shall:
- 176 (a) participate in cybersecurity information sharing initiatives coordinated by the Cyber  
177 Center;  
178 (b) designate a primary point of contact for cybersecurity matters who shall interface  
179 with the Cyber Center, the state board, and UETN; and  
180 (c) cooperate with statewide cybersecurity assessments and improvement initiatives.
- 181 (5)(a) A regional education service agency, as that term is defined in Section 53G-4-410,  
182 may serve as the designated primary cybersecurity contact for multiple LEAs within  
183 the service area.
- 184 (b) If a regional education service agency serves as the primary contact under Subsection  
185 (5)(a), the agency shall:
- 186 (i) coordinate with the Cyber Center, the state board, and UETN on behalf of the  
187 participating LEAs;  
188 (ii) ensure each participating LEA meets the minimum cybersecurity standards  
189 established under Subsection 63C-27-202(9); and  
190 (iii) maintain documentation of cybersecurity services provided to each LEA.
- 191 Section 5. Section **63C-27-201** is amended to read:
- 192 **63C-27-201 (Effective 05/06/26) (Repealed 07/01/32). Cybersecurity Commission**  
193 **created.**
- 194 (1) There is created the Cybersecurity Commission.
- 195 (2) The commission shall be composed of [24] the following members:
- 196 (a) one member the governor designates to serve as the governor's designee;  
197 (b) the commissioner of the Department of Public Safety;  
198 (c) the lieutenant governor, or an election officer, as that term is defined in Section

- 199 20A-1-102, the lieutenant governor designates to serve as the lieutenant governor's  
200 designee;
- 201 (d) the chief information officer of the Division of Technology Services;
- 202 (e) the chief information security officer, as described in Section 63A-16-210;
- 203 (f) the chairman of the Public Service Commission shall designate a representative with  
204 professional experience in information technology or cybersecurity;
- 205 (g) the executive director of the Utah Department of Transportation shall designate a  
206 representative with professional experience in information technology or  
207 cybersecurity;
- 208 (h) the director of the Division of Finance shall designate a representative with  
209 professional experience in information technology or cybersecurity;
- 210 (i) the executive director of the Department of Health and Human Services shall  
211 designate a representative with professional experience in information technology or  
212 cybersecurity;
- 213 (j) the director of the Division of Indian Affairs shall designate a representative with  
214 professional experience in information technology or cybersecurity;
- 215 (k) the Utah League of Cities and Towns shall designate a representative with  
216 professional experience in information technology or cybersecurity;
- 217 (l) the Utah Association of Counties shall designate a representative with professional  
218 experience in information technology or cybersecurity;
- 219 (m) the attorney general, or the attorney general's designee;
- 220 (n) the commissioner of financial institutions, or the commissioner's designee;
- 221 (o) the executive director of the Department of Environmental Quality shall designate a  
222 representative with professional experience in information technology or  
223 cybersecurity;
- 224 (p) the executive director of the Department of Natural Resources shall designate a  
225 representative with professional experience in information technology or  
226 cybersecurity;
- 227 (q) two local education agency employees tasked with job duties that include systems  
228 and security management from one charter school and one school district whom the  
229 state superintendent selects;
- 230 [(q)] (r) the highest ranking information technology official, or the official's designee,  
231 from each of:
- 232 (i) the Judicial Council;

- 233 (ii) the Utah Board of Higher Education;
- 234 (iii) the State Board of Education; and
- 235 (iv) the State Tax Commission;
- 236 ~~[(†)]~~ (s) the governor shall appoint:
- 237 (i) one representative from the Utah National Guard; and
- 238 (ii) one representative from the Governor's Office of Economic Opportunity;
- 239 ~~[(s)]~~ (t) the president of the Senate shall appoint one member of the Senate; and
- 240 ~~[(†)]~~ (u) the speaker of the House of Representatives shall appoint one member of the
- 241 House of Representatives.
- 242 (3)(a) The governor's designee shall serve as cochair of the commission.
- 243 (b) The commissioner of the Department of Public Safety shall serve as cochair of the
- 244 commission.
- 245 (4)(a) The members described in Subsection (2) shall represent urban, rural, and
- 246 suburban population areas.
- 247 (b) No fewer than half of the members described in Subsection (2) shall have
- 248 professional experience in cybersecurity or in information technology.
- 249 (5) In addition to the membership described in Subsection (2), the commission shall seek
- 250 information and advice from state and private entities with expertise in critical
- 251 infrastructure.
- 252 (6) As necessary to improve information and protect potential vulnerabilities, the
- 253 commission shall seek information and advice from federal entities including:
- 254 (a) the Cybersecurity and Infrastructure Security Agency;
- 255 (b) the Federal Energy Regulatory Commission;
- 256 (c) the Federal Bureau of Investigation; and
- 257 (d) the United States Department of Transportation.
- 258 (7)(a) Except as provided in Subsections (7)(b) and (c), a member is appointed for a
- 259 term of four years.
- 260 (b) A member shall serve until the member's successor is appointed and qualified.
- 261 (c) Notwithstanding the requirements of Subsection (7)(a), the governor shall, at the
- 262 time of appointment or reappointment, adjust the length of terms to ensure that the
- 263 terms of commission members are staggered so that approximately half of the
- 264 commission members appointed under Subsection ~~[(2)(†)]~~ (2) are appointed every two
- 265 years.
- 266 (8)(a) If a vacancy occurs in the membership of the commission, the member shall be

- 267 replaced in the same manner in which the original appointment was made.
- 268 (b) An individual may be appointed to more than one term.
- 269 (c) When a vacancy occurs in the membership for any reason, the replacement shall be
- 270 appointed for the unexpired term.
- 271 (9)(a) A majority of the members of the commission is a quorum.
- 272 (b) The action of a majority of a quorum constitutes an action of the commission.
- 273 (10) The commission shall meet at least two times a year.
- 274 Section 6. Section **63C-27-202** is amended to read:
- 275 **63C-27-202 (Effective 05/06/26) (Repealed 07/01/32). Commission duties.**
- 276 The commission shall:
- 277 (1) identify and inform the governor of:
- 278 (a) cyber threats and vulnerabilities towards Utah's critical infrastructure;
- 279 (b) cybersecurity assets and resources; and
- 280 (c) an analysis of:
- 281 (i) current cyber incident response capabilities;
- 282 (ii) potential cyber threats; and
- 283 (iii) areas of significant concern with respect to:
- 284 (A) vulnerability to cyber attack; or
- 285 (B) seriousness of consequences in the event of a cyber attack;
- 286 (2) provide resources with respect to cyber attacks in both the public and private sector,
- 287 including:
- 288 (a) best practices;
- 289 (b) education; and
- 290 (c) mitigation;
- 291 (3) promote cyber security awareness;
- 292 (4) share information;
- 293 (5) promote best practices to prevent and mitigate cyber attacks;
- 294 (6) enhance cyber capabilities and response for all Utahns;
- 295 (7) provide consistent outreach and collaboration with private and public sector
- 296 organizations;~~and~~
- 297 (8) share cyber threat intelligence to operators and overseers of Utah's critical infrastructure~~[-]~~
- 298 ; and
- 299 (9) in accordance with Title 63G, Chapter 3, Utah Administrative Rulemaking Act, make
- 300 rules establishing minimum cybersecurity standards for a local education agency, as that

- 301 term is defined in Section 53G-3-402, that:
- 302 (a) align with industry recognized cybersecurity frameworks and standards, including  
303 frameworks developed by the National Institute of Standards and Technology, the  
304 Center for Internet Security, or a successor organization;
- 305 (b) take into account varying local education agency resources, capacity, and needs;
- 306 (c) establish phased implementation timelines based on local education agency size,  
307 existing cybersecurity infrastructure, and available resources; and
- 308 (d) as appropriate based on the local education agency's size, risk profile, and available  
309 resources, shall address:
- 310 (i) identity and access management;
- 311 (ii) asset management and inventory of hardware, software, and data systems;
- 312 (iii) data protection;
- 313 (iv) security monitoring and logging capabilities;
- 314 (v) vulnerability management, including regular security assessments and patching  
315 procedures;
- 316 (vi) incident response and recovery planning;
- 317 (vii) security awareness training requirements for staff and administrators;
- 318 (viii) third-party risk management for vendors with access to local education agency  
319 systems or data;
- 320 (ix) network security controls;
- 321 (x) backup and disaster recovery procedures; and
- 322 (xi) governance structures for cybersecurity oversight within a local education  
323 agency.

324 **Section 7. Effective Date.**

325 This bill takes effect on May 6, 2026.

326 **Section 8. Coordinating H.B. 42 with S.B. 69.**

327 If H.B. 42, School Cybersecurity Amendments, and S.B. 69, School Device Revisions,  
328 both pass and become law, the Legislature intends that, on July 1, 2026, Subsection  
329 53G-7-227(2) enacted in S.B. 69, be amended to read:

330 "(2) Except as provided in Subsection (3), a student may not use a cellphone, smart watch,  
331 AI glasses, or emerging technology at a school during school hours."