



# Digital Safety Bill

Utah Attorney General  
Youth Advisory Committee

Presented by:  
Joyce Wang and Anh Khoa Le

# Current Problem



The current curriculum only has one (1) standard that **covers online safety**. (Standard 2 of strand 4 on the digital literacy CTE curriculum.)

Current requirements make digital welfare and literacy up to school districts, making **curriculums too inconsistent**.

Of the topics covered in online safety in the Digital Literacy CTE course, many pertinent **sensitive topics are often disregarded**. (e.g. online sex trafficking, sexting, pornography)

The culture has changed and many **teachers are unfamiliar** with the current online world, making it difficult to teach.

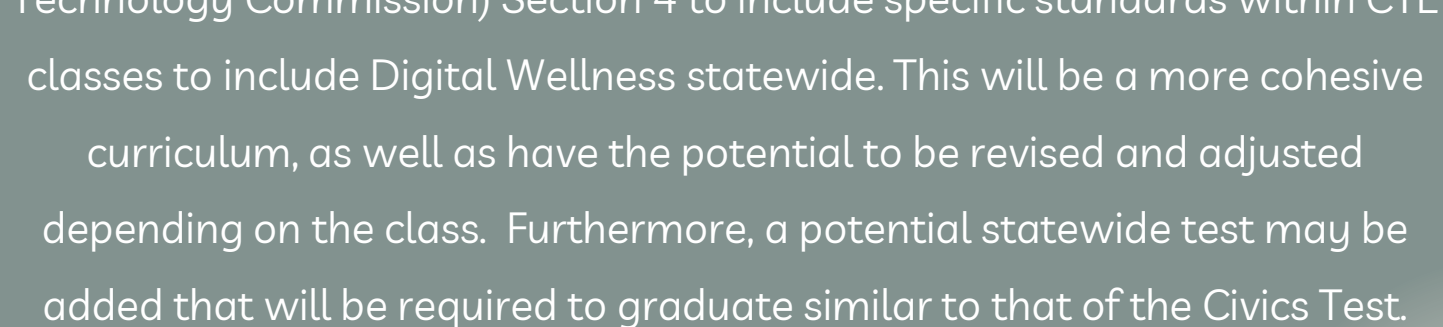




# Main Idea

---

We plan to amend H.B. 372 (Digital Wellness, Citizenship, and Safe Technology Commission) Section 4 to include specific standards within CTE classes to include Digital Wellness statewide. This will be a more cohesive curriculum, as well as have the potential to be revised and adjusted depending on the class. Furthermore, a potential statewide test may be added that will be required to graduate similar to that of the Civics Test.



## Standard 2

Demonstrate knowledge of online safety, digital security, and online privacy.

- Define **online safety** as being aware of online risks and maximizing the user's personal safety.
- Identify guidelines to protect users from various types of online predators.
  - Avoid using suggestive screen names or photos.
  - Be aware of excessive attention.
  - Do not talk to anyone that wants to get too personal.
  - Keep in mind that people are not always who they say they are.
  - Never arrange to meet with someone you only know online in person.
  - Tell a trusted adult if you encounter a problem.
- Define **digital security** as tools used to secure identify and data online.
- Identify threats in the digital world.
  - Define **adware** as software that automatically displays unwanted advertising material when a user in online (i.e. pop-up advertisements)
  - Define **computer worm virus** as a malicious software that replicates itself to spread to other digital devices through a network.

# Curriculum

This includes the current strands and standards included within the Digital Literacy curriculum.

- Define **denial of service attacks** as an attack to shut down a computer device or network by flooding it with traffic to make it inaccessible to the intended users.
- Define **hackers** as a person or program that uses computers to gain unauthorized access to data.
- Define **malware** as software that is specifically designed to disrupt, damage, or gain unauthorized access to a digital device.
- Define **ransomware** as a type of malicious software that is used to block access to a digital device until a sum of money is paid.
- Define **spyware** as software that enables a user to obtain private information about another's computer activity by transmitting data secretly from their hard drive.
- Define **Trojan Horse** as a malicious code that looks legitimate and takes control of your computer to damage, disrupt, and destroy your data.
- Explain the importance of using anti-virus protection software on your digital device.
  - Define **anti-virus protection software** as software designed to protect your computing device and destroy computer viruses.
- Define **online privacy** as the protection of private data and communication.
- Identify threats to online transactions.
  - Browser extensions
  - Credit card fraud
  - Data misuse
  - Hacking
  - Money theft
  - Unprotective services
- Identify threats to email and online communication.
  - Catfishing
  - Email scams
  - Hacking
  - Phishing attacks
  - Spoofing
- Explain the importance of different security measures on your digital devices.
  - Password/passphrase
  - Two-factor authentication
  - Firewalls
  - Secure website (HTTPS)
  - Updates



# Specific Standards to add into CTE

01

## Digital Wellness

Students are able to stay healthy within the internet and learn the difference between what goes on within the internet and real life.

02

## Staying Safe

Practice responsible ways to communicate online, via text, or through other electronic means and how to respond to inappropriate contact or sexual advances online, via text, or through other electronic means.

03

## Positive Behaviors Plan

Reinforce positive behavior online to combat rising issues such as suicide and cyberbullying through programs such as QPR training.

04

## Internet Identity

Evaluate the importance of the separation of an online and offline identity, as well as staying away from unsecured sites, unknown links, various viruses, etc.



# Bill

Section 4. Section 63C-21-202 is enacted to read:

102 63C-21-202. Commission duties -- Reporting requirements.

103 (1) To ensure students are digital media-literate, and able to use technology safely and  
104 ethically, the commission shall:

105 (a) identify best practices for reaching every student with training in digital citizenship;

106 (b) identify, compile, and publish resources that an LEA or a parent may use to educate  
107 students, parents, or a student's support network in digital citizenship;

108 (c) identify and compile emerging research on digital citizenship and educating  
109 students, parents, or a student's support network in digital citizenship;

110 (d) collaborate and coordinate efforts with programs related to cyber-bullying, suicide  
111 prevention, anti-pornography, and social and emotional learning to provide resources for  
112 promoting digital citizenship to LEAs, students, teachers, and parents;

113 (e) administer funds appropriated by the Legislature for the purposes described in this  
114 part, in accordance with the intent of the Legislature for the appropriation;

(f) regulate a cohesive statewide curriculum covering standards as suggested by the Digital  
Wellness, Citizenship, and Safety Technology Commission; and

(g) provide a mandated statewide test that will be necessary to graduate covering core digital  
literacy and welfare standards.

115 (2) The commission shall annually report to the Education Interim Committee and the  
116 state board on:

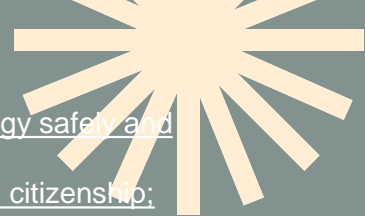
117 (a) objectives for training students in digital citizenship within the CTE curriculum specific to  
digital wellness, staying safe, positive behaviours plan and internet identity;

118 (b) a template for a plan that an LEA may use to achieve the objectives described in  
119 Subsection (2)(a);

120 (c) involving parents in promoting digital citizenship, including resources for educating  
121 students and parents at home;

122 (d) approved providers to deliver training in digital citizenship to teachers and students  
123 in LEAs; and

124 (e) the expenditure of the funds described in Subsection (1)(e).





Thank you for your  
time!

Do you have any questions?

