H-4379.1

1 2

3

4 5

6

SECOND SUBSTITUTE HOUSE BILL 2823

State of Washington 64th Legislature 2016 Regular Session

By House Appropriations (originally sponsored by Representatives Parker, Riccelli, Manweller, and Bergquist)

READ FIRST TIME 02/09/16.

AN ACT Relating to creating a program to provide students and the community with the means to report anonymously concerning unsafe or violent activities, or the threat of these activities; reenacting and amending RCW 42.56.240; adding a new section to chapter 28A.300 RCW; adding a new section to chapter 28A.320 RCW; creating a new section; and prescribing penalties.

- 7 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:
- The legislature finds that violence in 8 NEW SECTION. Sec. 1. 9 schools is a serious concern. The legislature intends to limit violence in schools by providing students and the community with a 10 11 mechanism to report anonymously information about potentially 12 dangerous situations.
- NEW SECTION. Sec. 2. A new section is added to chapter 28A.300 RCW to read as follows:
- 15 (1) The students protecting students program is established 16 within the office of the superintendent of public instruction. The 17 primary purpose of the statewide program is to provide students and 18 the community with the means to relay information anonymously 19 concerning unsafe, potentially harmful, dangerous, violent, or 20 criminal activities, or the threat of these activities, to school

p. 1 2SHB 2823

officials or, if necessary, appropriate law enforcement or public safety agencies.

(2) The students protecting students program must:

- (a) Establish and maintain methods of anonymous reporting concerning unsafe, potentially harmful, dangerous, violent, or criminal activities, or the threat of these activities, where reporting can be accomplished by, at a minimum, phone, text message, and email;
- (b) Establish methods and procedures, consistent with the federal health insurance portability and accountability act and the federal educational rights and privacy act, to ensure that the identity of the reporting party remains unknown to persons and entities, including employees or persons operating the program, law enforcement officers, public safety officers, and school officials;
- (c) Establish methods and procedures so that information obtained from a reporting party who voluntarily discloses his or her identity and verifies that he or she is willing to be identified may be shared with employees or persons operating the program, law enforcement officers, public safety officers, and school officials;
- (d) Establish methods and procedures to ensure that the identity of a reporting party who becomes known through any means other than voluntary disclosure is not further disclosed; and
- (e) Promptly forward information received by the program to the appropriate law enforcement or public safety agency or school officials.
- (3) The identity of the reporting party or other personally identifiable information may be released by the students protecting students program to a school district or law enforcement officer when that school district superintendent or law enforcement officer declares in an affidavit that after a threat assessment or other investigation of the report he or she has probable cause to believe that the reporting party knowingly filed a fraudulent report. The superintendent of public instruction must approve the release of the identity or other personally identifiable information by the students protecting students program under this subsection.
- (4) The office of the superintendent of public instruction must contract with an organization or call center to provide the program described in this section. The organization or call center must have the ability to receive anonymous reporting from students and the community twenty-four hours per day, seven days per week, and the

p. 2 2SHB 2823

ability to promptly forward the information as required in this section.

- (5)(a) The students protecting students program and employees or persons operating the program must not be compelled to produce any personally identifiable information except on the motion of a criminal defendant to the court in which the offense is being tried, supported by an affidavit establishing that the personally identifiable information contains impeachment evidence or evidence that is exculpatory to the defendant in the trial of that offense.
- (b) If the defendant's motion is granted, the court shall conduct an ex parte in camera review of personally identifiable information produced under the defendant's subpoena.
- (c) If the court determines that the produced personally identifiable information contains impeachment evidence or evidence that is exculpatory to the defendant, the court shall order the personally identifiable information be produced to the defendant pursuant to a protective order that includes the redaction of the reporting party's identity and limitations on the use of the personally identifiable information, as needed, unless contrary to state or federal law. Personally identifiable information excised pursuant to a judicial order following the in camera review must be sealed and preserved in the records of the court, to be made available to the appellate court in the event of an appeal. After the time for appeal has expired, the court must return the personally identifiable information to the students protecting students program.
- (6)(a) Personally identifiable information created or obtained through the implementation or operation of the students protecting students program is confidential and must not be disclosed. The students protecting students program and employees or persons operating the program may be compelled to produce personally identifiable information only before a court or other tribunal and only pursuant to court order for an in camera review. An in camera review must be limited to an inspection of personally identifiable information that is material to the specific case pending before the court. The attorney general acting on behalf of the students protecting students program has standing in an action to oppose the disclosure of personally identifiable information in the custody of the program.
- (b) An employee or person operating the program who knowingly discloses personally identifiable information in violation of the

p. 3 2SHB 2823

- 1 provisions of this section commits a misdemeanor punishable under 2 chapter 9A.20 RCW.
- 3 (7) The definitions in this subsection apply throughout this 4 section unless the context clearly requires otherwise.
- 5 (a) "In camera" means a confidential review by the judge alone in 6 his or her chambers.
- 7 (b) "Personally identifiable information" means the name of the 8 reporting party; the address, phone number, or email address of the 9 reporting party; personal indirect identifiers of the reporting 10 party, such as social security number, student number, date of birth, 11 mother's maiden name; or other information that, alone or in 12 combination, with other information, could be used to determine the 13 identity of the reporting party.
- NEW SECTION. Sec. 3. A new section is added to chapter 28A.320 RCW to read as follows:

16

17

18

19 20

21

22

2324

25

2627

28

2930

31

32

- (1) Every school year, beginning in the 2016-17 school year, there must be made available to all students in each common school as defined in RCW 28A.150.020 at least one age-appropriate educational program, class, or activity designed to teach students about the students protecting students program established in section 2 of this act. Such a program, class, or activity must include information about how to report anonymously concerning unsafe, potentially harmful, dangerous, violent, or criminal activities, or the threat of these activities, to appropriate law enforcement agencies, public safety agencies, and school officials.
- (2) Beginning in the 2016-17 school year, schools and school districts must disseminate information about the students protecting students program established in section 2 of this act, including the contact information for anonymous reporting, through any normal means of existing communication to students and families.
- **Sec. 4.** RCW 42.56.240 and 2015 c 224 s 3 and 2015 c 91 s 1 are each reenacted and amended to read as follows:
- The following investigative, law enforcement, and crime victim information is exempt from public inspection and copying under this chapter:
- 36 (1) Specific intelligence information and specific investigative 37 records compiled by investigative, law enforcement, and penology 38 agencies, and state agencies vested with the responsibility to

p. 4 2SHB 2823

discipline members of any profession, the nondisclosure of which is essential to effective law enforcement or for the protection of any person's right to privacy;

- (2) Information revealing the identity of persons who are witnesses to or victims of crime or who file complaints with investigative, law enforcement, or penology agencies, other than the commission, if disclosure would endanger any person's life, physical safety, or property. If at the time a complaint is filed the complainant, victim, or witness indicates a desire for disclosure or nondisclosure, such desire shall govern. However, all complaints filed with the commission about any elected official or candidate for public office must be made in writing and signed by the complainant under oath;
- (3) Any records of investigative reports prepared by any state, county, municipal, or other law enforcement agency pertaining to sex offenses contained in chapter 9A.44 RCW or sexually violent offenses as defined in RCW 71.09.020, which have been transferred to the Washington association of sheriffs and police chiefs for permanent electronic retention and retrieval pursuant to RCW 40.14.070(2)(b);
- 20 (4) License applications under RCW 9.41.070; copies of license 21 applications or information on the applications may be released to 22 law enforcement or corrections agencies;
 - (5) Information revealing the identity of child victims of sexual assault who are under age eighteen. Identifying information means the child victim's name, address, location, photograph, and in cases in which the child victim is a relative or stepchild of the alleged perpetrator, identification of the relationship between the child and the alleged perpetrator;
 - (6) Information contained in a local or regionally maintained gang database as well as the statewide gang database referenced in RCW 43.43.762;
- 32 (7) Data from the electronic sales tracking system established in 33 RCW 69.43.165;
 - (8) Information submitted to the statewide unified sex offender notification and registration program under RCW 36.28A.040(6) by a person for the purpose of receiving notification regarding a registered sex offender, including the person's name, residential address, and email address;
- 39 (9) Personally identifying information collected by law 40 enforcement agencies pursuant to local security alarm system programs

p. 5 2SHB 2823

- 1 and vacation crime watch programs. Nothing in this subsection shall
- 2 be interpreted so as to prohibit the legal owner of a residence or
- 3 business from accessing information regarding his or her residence or
- 4 business;

7

8

9

10 11

12

13

14

1516

17

18

19

- 5 (10) The felony firearm offense conviction database of felony 6 firearm offenders established in RCW 43.43.822;
 - (11) The identity of a state employee or officer who has in good faith filed a complaint with an ethics board, as provided in RCW 42.52.410, or who has in good faith reported improper governmental action, as defined in RCW 42.40.020, to the auditor or other public official, as defined in RCW 42.40.020;
 - (12) The following security threat group information collected and maintained by the department of corrections pursuant to RCW 72.09.745: (a) Information that could lead to the identification of a person's security threat group status, affiliation, or activities; (b) information that reveals specific security threats associated with the operation and activities of security threat groups; and (c) information that identifies the number of security threat group members, affiliates, or associates; ((and))
- 20 (13) The global positioning system data that would indicate the 21 location of the residence of an employee or worker of a criminal 22 justice agency as defined in RCW 10.97.030; and
- 23 (14) Personally identifiable information, as defined in section 2 24 of this act, received, made, or kept by, or received from, the 25 students protecting students program established in section 2 of this 26 act, that is confidential under section 2(6) of this act.

--- END ---

p. 6 2SHB 2823