..... moves to amend H.F. No. 2898 as follows:

Delete everything after the enacting clause and insert:

"Section 1. **[125B.30] CITATION.**

Sections 125B.30 to 125B.37 may be cited as the "Minnesota Student Data Privacy Act."

Sec. 2. **[125B.31] DEFINITIONS.**

(a) For the purposes of sections 125B.30 to 125B.37, the following terms have the meanings given them.

(b) "1-to-1 program" means any program authorized by an educational institution where a technological device is provided to a student by or through an educational institution for overnight or at-home use.

(c) "1-to-1 device" means a technological device provided to a student pursuant to a 1-to-1 program.

(d) "1-to-1 device provider" means a person or entity that provides a 1-to-1 device to a student or educational institution pursuant to a 1-to-1 program, and includes any business or nonprofit entities that share a parent, subsidiary, or sister relationship with the entity that provides the 1-to-1 device.

(e) "Aggregate data" means student-related data collected and reported by an educational institution at the group, cohort, or institutional level that contains no personally identifiable student information.

(f) "De-identified" means having removed or obscured any personally identifiable information from personally identifiable student information in a manner that prevents the unintended disclosure of the identity of the student or information about the student. Information shall not be considered de-identified if it meets the definition of "personally identifiable student information" in paragraph (o).

(g) "Educational institution" means:

(1) a school under section 120A.22, subdivision 4, excluding a home school, and also includes public postsecondary institutions and private postsecondary institutions subject to registration or licensure under chapter 136A or 141; or

(2) a state or local educational agency authorized to direct or control an entity in clause (1).

(h) "Educational data" has the meaning given under section 13.32, subdivision 1, paragraph (a).

(i) "Education research" means the systematic gathering of empirical information to advance knowledge, answer questions, identify trends, or improve outcomes within the field of education.

(j) "Elementary school" has the meaning given under section 120A.05, subdivision 9.

(k) "Law enforcement official" means a peace officer or a school resource officer under sections 121A.40 to 121A.56.

(l) "Location tracking technology" means any hardware, software, or application that collects or reports data that identifies the geophysical location of a technological device.

(m) "Opt-in agreement" means a discrete, verifiable, written, or electronically generated agreement by which, subject to the provisions of sections 125B.30 to 125B.37, a student's parent or guardian, or an adult student defined as an eligible student under federal law, voluntarily grants a school employee, SIS provider, or 1-to-1 device provider with limited permission to access and interact with a specifically defined set of personally identifiable student information.

(n) "Personal technological device" means a technological device owned, leased, or otherwise lawfully possessed by a student that is not a 1-to-1 device.

(o) "Personally identifiable student information" means one or more of the following:

(1) a student's name;

(2) the name of a student's parent, legal guardian, or other family member;

(3) the address of a student or student's parent, legal guardian, or other family member;

(4) a photograph, video, or audio recording that contains the student's image or voice;

(5) indirect identifiers, including but not limited to a student's date of birth, place of birth, mother's maiden name, Social Security number, student number, biometric record, telephone number, credit card account number, insurance account number, financial services account number, customer number, persistent online identifier, e-mail address, social media address, or other electronic address;

(6) any aggregate or de-identified student data that is capable of being disaggregated or reconstructed to the point that individual students can be identified; and

(7) any student data or other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person who does not have personal knowledge of the relevant circumstances to identify a specific student with reasonable certainty.

(p) "School employee" means all individuals employed in a school and all individuals who provide services to a school as a volunteer, contractor, or under another agreement.

(q) "SIS provider" means an entity that sells, leases, provides, operates, or maintains a student information system for the benefit of an educational institution.

(r) "Student" means a person enrolled in a school under section 120A.22.

(s) "Student data" means educational data under section 13.32 that is collected and stored by an educational institution, or by a person or entity acting on behalf of that institution, and included in a student's educational data.

(t) "Student information system" or "SIS" means a software application or cloud-based service that allows an educational institution to input, maintain, manage, or retrieve student data or personally identifiable student information, including applications that track or share personally identifiable student information in real time.

(u) "Technological device" means any computer, cellular phone, smartphone, digital camera, video camera, audio recording device, or other electronic device that can be used for creating, storing, or transmitting information in the form of electronic data.

Sec. 3. **[125B.32] STUDENT INFORMATION SYSTEMS.**

Subdivision 1. **Student information system contracts; requirements; prohibitions.** (a) Any contract or other agreement between an educational institution and an SIS provider pursuant to which the SIS provider sells, leases, provides, operates, or maintains an SIS for the benefit of the educational institution shall expressly authorize and require the SIS provider to:

(1) establish, implement, and maintain appropriate security measures, consistent with current best practices, to protect the student data and personally identifiable student information the SIS provider creates, sends, receives, stores, and transmits in conjunction with the operation of the student information system;

(2) acknowledge that no data stored on the student information system is the property of the SIS provider;

(3) establish and implement policies and procedures for responding to data breaches involving the unauthorized acquisition of or access to any personally identifiable student information on the student information system. Such policies and procedures, at a minimum, shall:

(i) require notice be provided by the SIS provider to any and all affected parties, including educational institutions, students, and students' parents and legal guardians, within 30 days of the discovery of the breach;

(ii) require the notice to include a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(iii) require the notice to provide a procedure by which affected parties may learn what types of sensitive personally identifiable information the SIS provider maintained about the affected individual; and

(iv) satisfy all other applicable breach notification standards established under state or federal law;

(4) permanently delete all data stored on the student information system, and destroy all nondigital records containing any personally identifiable student information retrieved from the student information system, within 90 days of the termination of the SIS provider's contact with the educational institution, except where the SIS provider and the person authorized to sign a valid opt-in agreement pursuant to subdivision 2 mutually agree the SIS provider will retain specifically identified data or nondigital records for the student's benefit. Prior to deletion, if requested by the educational institution, the terminated SIS provider shall transfer a designated portion or all of the data stored on the student information system to another designated SIS provider at the educational institution's expense; and

(5) comply with all the applicable obligations and restrictions established for SIS providers in sections 125B.30 to 125B.37.

(b) A contract or other agreement under paragraph (a) shall expressly prohibit the SIS provider from:

(1) analyzing, interacting with, sharing, or transferring any student data or personally identifiable student information the educational institution inputs into or otherwise provides to the student information system unless:

(i) permission to do so has been granted under an opt-in agreement under subdivision 2;

(ii) the SIS provider analyzes or interacts with the student data or personally identifiable student information:

(A) in order to meet a contractual obligation to the educational institution; and

(B) any analysis of or interaction with the data or information is limited to meeting that contractual obligation;

(iii) the SIS provider analyzes or interacts with the student data or personally identifiable student information:

(A) in response to a specific request made by an educational institution; and

(B) any data or information produced as a result of the analysis or interaction is limited to the educational purpose for which it was sought;

(iv) the educational institution determines, and documents in writing, that sharing specific student data or personally identifiable student information is necessary to safeguard students' health or safety while students are traveling to or from the educational institution, are on the educational institution's property, or are participating in an event or activity supervised by the educational institution;

(v) at the request of the educational institution, the SIS provider de-identifies or aggregates student data or personally identifiable student information for the purpose of:

(A) enabling the educational institution to comply with federal, state, or local reporting and data-sharing requirements; or

(B) education research; or

(vi) the data is accessed by the SIS provider for the exclusive purpose of testing and improving the value and performance of its student information system for the benefit of the educational institution. Where data is accessed to test and improve student information system value and performance:

(A) any copied data shall be permanently deleted within 60 days of the date the copy was created; and

(B) any data analysis that contains personally identifiable student information shall be permanently deleted within 60 days of the date the analysis was created;

(2) selling any student data or personally identifiable student information stored on or retrieved from the student information system unless it is sold as part of a sale or merger of the entirety of the SIS provider's business. Upon such a sale or merger, the provisions of sections 125B.30 to 125B.37, and any relevant contracts or agreements, shall apply fully to the new purchasing or controlling person or entity; and

(3) using any student data or personally identifiable student information stored on or retrieved from the student information system to inform, influence, or guide marketing or advertising efforts directed at a student, a student's parent or legal guardian, or a school employee, except pursuant to a valid opt-in agreement; and

(4) using any student data or personally identifiable student information stored on or retrieved from the student information system to develop, in whole or in part, a profile of a student or group of students for any commercial or other noneducational purposes.

Subd. 2. **Opt-in agreements.** (a) A valid opt-in agreement shall identify, with specificity:

(1) the precise subset of personally identifiable student information in the student information system, which may include student attendance records and student disciplinary records, as to which the SIS provider is being granted authority to access, analyze, interact with, share, or transfer;

(2) the name of the SIS provider to whom the authority to access, analyze, interact with, share, or transfer personally identifiable student information in the student information system is being granted;

(3) the educational purpose for which the authority to access, analyze, interact with, share, or transfer personally identifiable student information is being granted; and

(4) the individual student to whom the opt-in agreement applies.

(b) An opt-in agreement shall only be valid if it has been signed by:

(1) the student's parent or guardian, if the student is in elementary school;

(2) the student and the student's parent or legal guardian, if the student has advanced beyond elementary school but has not yet reached the age of majority; or

(3) the student alone, if the student has reached the age of majority.

(c) A valid opt-in agreement may authorize an SIS provider to share or transfer personally identifiable student information to another person or entity only where:

(1) the purpose of the transfer of the personally identifiable student information is to benefit:

(i) the operational, administrative, analytical, or educational functions of the educational institution, including education research; or

(ii) the student's education;

(2) the subset of personally identifiable student information to be shared or transferred is identified with specificity in the opt-in agreement;

(3) the person or entity to whom the personally identifiable student information is being shared or transferred is identified with specificity in the opt-in agreement;

(4) the benefit to the educational institution or student is identified with specificity in the opt-in agreement; and

(5) for each student, a record of what specific personally identifiable student information pertaining to that student was shared or transferred, when it was shared or transferred, and with whom it was shared or transferred is appended to the student's record.

(d) Any person or entity that accesses or takes possession of any student data or personally identifiable student information under subdivision 1, paragraph (b), clause (1), item (i); or clause (2), shall be subject to the same restrictions and obligations under this

section as the SIS provider from which the student data or personally identifiable student information was obtained.

(e) An opt-in agreement shall not be valid if it grants general authority to access, analyze, interact with, share, or transfer a student's personally identifiable student information in a student information system.

(f) Except as authorized in this section, no SIS provider, school employee, or other person or entity who receives personally identifiable student information, directly or indirectly, from a student information system pursuant to an opt-in agreement may share, sell, or otherwise transfer such information to another person or entity.

(g) An opt-in agreement may be revoked at any time, upon written notice to an educational institution, by the person eligible to authorize an opt-in agreement under paragraph (b). Within 30 days of such a revocation, notice to the SIS provider shall be provided by the educational institution.

(h) An SIS provider that accesses, analyzes, interacts with, shares, or transfers personally identifiable student information to another person or entity shall bear the burden of proving that it acted pursuant to a valid opt-in agreement.

(i) No educational benefit may be withheld from, or punitive measure taken against, a student or the student's parent or legal guardian based in whole or in part upon a decision not to sign, or to revoke, an opt-in agreement.

Subd. 3. **School employees.** (a) Subject to written authorization from the educational institution, school employees may access and interact with student data and personally identifiable student information on a student information system in furtherance of their professional duties. Notwithstanding any other provisions in this section, no school employee may receive authorization to access and interact with student data or personally identifiable student information on a student information system until the employee has received adequate training to ensure the school employee's understanding and compliance with the provisions of this section.

(b) School employees may not sell, share, or otherwise transfer student data or personally identifiable student information to another person or entity, except:

(1) where specifically authorized to do so pursuant to this section;

(2) with the educational institution that employs the school employee;

(3) with another school employee who is eligible to access such information pursuant to paragraph (a); or

(4) where:

(i) the school employee is a teacher;

(ii) the teacher is transferring student data to a software application for classroom record keeping or management purposes only;

(iii) any third parties with access to the software application are expressly prohibited from reviewing or interacting with the transferred data; and

(iv) any data transferred to the software application by the teacher is deleted by the teacher within 45 days of such time as it is no longer being actively used for classroom record keeping or management purposes.

Subd. 4. **Parent or guardian access to student data.** (a) A student's parent or guardian, upon written request to an educational institution, shall be permitted to inspect and review the child's student data and personally identifiable student information that is stored on a student information system. Educational institutions shall afford parents and legal guardians a reasonable and fair opportunity to request corrections to or seek removal of inaccurate data.

(b) The right of a student's parent or guardian to review the child's student data and personally identifiable student information shall not apply where:

(1) such information was supplied by the child to the educational institution; and

(2) there is a reasonable likelihood the disclosure of such information would generate a threat to the student's health or safety.

(c) The right of a student's parent or guardian to review their child's student data and personally identifiable student information shall not apply where access to particularly specified information has been waived by the student or the student's parent or guardian.

(d) When a student reaches the age of majority, the rights granted to a student's parents and legal guardian pursuant to this subdivision shall terminate and instead shall vest with the student.

(e) An educational institution shall establish appropriate procedures for:

(1) reviewing and responding to requests made pursuant to this subdivision within 30 days of its receipt of the request; and

(2) requesting and receiving a fair hearing in the event a requested correction is denied.

Subd. 5. **Requirements for deletion of data in student information systems.** One year after a student's graduation, withdrawal, or expulsion from an educational institution, all student data and personally identifiable student information related to that student that is stored in a student information system shall be deleted. This provision shall not apply to:

(1) a student's name and Social Security number;

(2) a student's transcript, graduation record, letters of recommendation, and other information required by an institution of higher education for an application for admission or by a potential employer for an application for employment;

(3) student data and personally identifiable student information that is the subject of an ongoing disciplinary, administrative, or judicial action or proceeding;

(4) de-identified student data that is being retained at the request of the educational institution for the purpose of educational research or analysis; and

(5) student data or personally identifiable student information where its retention is otherwise required by law or a judicial order or warrant.

Subd. 6. **Requirements for deletion of physical or digital copies of student data.** Within 180 days of receiving notification, pursuant to subdivision 7, of a student's graduation, withdrawal, or expulsion from an educational institution, all physical or digital copies of any student data and personally identifiable student information related to the student that was obtained from a student information system and is in the possession or under the control of an SIS provider or other third party shall be deleted or destroyed. This provision shall not apply to:

(1) student data and personally identifiable student information that is the subject of an ongoing disciplinary, administrative, or judicial action or proceeding;

(2) aggregated or de-identified student data obtained for the purpose of education research;

(3) student data or personally identifiable student information where its retention is otherwise required by law or a judicial order or warrant; and

(4) specifically identified student data or personally identifiable student information, where:

(i) its retention is requested by the person authorized to sign a valid opt-in agreement pursuant to subdivision 2, paragraph (b); and

(ii) the SIS provider and educational institution voluntarily consent to its retention.

Subd. 7. **Notice to SIS provider and third parties.** Within 90 days of a student's graduation, withdrawal, or expulsion from an educational institution, notice of such shall be provided by the educational institution to the SIS provider, which shall in turn notify any third parties with whom the SIS provider shared the student's student data or personally identifiable student information.

Subd. 8. **Access under law, judicial warrant, or audit.** No person or entity, other than an educational institution, school employee, or SIS provider, other than as provided for in this section, shall be granted access to review or interact with a student information

system and the data thereon, unless otherwise authorized to do so by law, pursuant to a judicial warrant, or as part of an audit initiated by an educational institution.

Subd. 9. **Directory information permitted.** Nothing in this section shall be read to prohibit an educational institution from providing directory information to a vendor for the express purpose of providing photography services, class ring services, yearbook or student publication publishing services, memorabilia services, or similar services, provided the vendor agrees in writing:

(1) not to sell or transfer the data to any other persons or entities;

(2) to use the data solely for the express purpose for which it was provided; and

(3) to destroy the data upon completion of its use for the express purpose for which it was provided.

Subd. 10. **Interaction with other law.** Nothing in this section shall be read to supersede or otherwise limit any laws that provide enhanced privacy protections to students or further restrict access to their educational data or personally identifiable student information.

Sec. 4. **[125B.33] 1-TO-1 PROGRAMS.**

Subdivision 1. **General rule.** When an educational institution or 1-to-1 device provider provides a student with a technological device pursuant to a 1-to-1 program, no school employee or 1-to-1 device provider, or an agent thereof, may access or track such a device or the activity or data thereupon, either remotely or in person, except in accordance with the provisions of this section.

Subd. 2. **Exceptions.** No school employee or 1-to-1 device provider, or an agent thereof, may access any data input into, stored upon, or sent or received by a student's 1-to-1 device, including but not limited to its browser, keystroke, or location history, nor may such data be analyzed, interacted with, shared, or transferred unless:

(1) the data being collected is not personally identifiable student information;

(2) the data is being accessed by or on behalf of a school employee who:

(i) is the student's teacher;

(ii) is receiving or reviewing the information for an educational purpose consistent with the teacher's professional duties; and

(iii) does not use the information, or permit any other person or entity to use the information, for any other purpose;

(3) a school employee or 1-to-1 device provider or an agent thereof has been authorized to access specific personally identifiable student information pursuant to an opt-in agreement under subdivision 9;

(4) a school employee has a reasonable suspicion that the student has violated or is violating an educational institution policy and that data on the 1-to-1 device contains evidence of the suspected violation, subject to the following limitations:

(i) prior to searching a student's 1-to-1 device based on reasonable individualized suspicion, the school employee shall document the reasonable individualized suspicion and notify the student and the student's parent or legal guardian of the suspected violation and what data will be accessed in searching for evidence of the violation. An educational institution, subject to any other relevant legal restrictions, may seize a student's 1-to-1 device to prevent data deletion pending notification, provided that:

(A) the prenotification seizure period is no greater than 48 hours; and

(B) the 1-to-1 device is stored securely on educational institution property and not accessed during the prenotification seizure period;

(ii) searches of a student's device based upon a reasonable individualized suspicion that an educational institution policy has been violated shall be strictly limited to finding evidence of the suspected policy violation and shall immediately cease upon finding sufficient evidence of the suspected violation. It shall be a violation of this item to copy, share, or transfer any data, or any information thereabout, that is unrelated to the specific suspected violation which prompted the search of the 1-to-1 device; and

(iii) when a student is suspected of illegal conduct, no search of the 1-to-1 device may occur unless a judicial warrant has been secured according to clause (5) even if the student is also suspected of a related or unrelated violation of educational institution policy;

(5) a school employee or law enforcement official reasonably suspects the student has engaged or is engaging in illegal conduct, reasonably suspects data on the 1-to-1 device contains evidence of the suspected illegal conduct, and has secured a judicial warrant for a search of the device;

(6) doing so is necessary to update or upgrade a device's software, or protect the device from cyberthreats, and access is limited to that purpose;

(7) doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose. Within 72 hours of accessing a 1-to-1 device's data in response to an imminent threat to life or safety, the school employee or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution with a written description of the precise threat that prompted the access and what data was accessed; or

(8) the information sent from the device is posted on a Web site that:

(i) is accessible by the general public; or

(ii) is accessible by a specific school employee who was granted permission by the student to view the content.

Subd. 3. **Use of location tracking technology.** No school employee or 1-to-1 device provider, or an agent thereof, may use a student's 1-to-1 device's location tracking technology to track a device's real-time or historical location, unless:

(1) such use is ordered pursuant to a judicial warrant;

(2) the student to whom the device was provided, or the student's parent or legal guardian, has notified a school employee or law enforcement official that the device is missing or stolen; or

(3) doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose. Within 72 hours of accessing a 1-to-1 device's location tracking technology in response to an imminent threat to life or safety, the school employee or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what data and features were accessed.

Subd. 4. **No access to audio or video receiving, transmitting, or recording functions; exceptions.** No school employee or 1-to-1 device provider, or an agent thereof, may activate or access any audio or video receiving, transmitting, or recording functions on a student's 1-to-1 device, unless:

(1) a student initiates a video chat or audio chat with the school employee or 1-to-1 device provider;

(2) the activation or access is ordered pursuant to a judicial warrant; or

(3) doing so is necessary in response to an imminent threat to life or safety and access is limited to that purpose. Within 72 hours of accessing a 1-to-1 device's audio or video receiving, transmitting, or recording functions in response to an imminent threat to life or safety, the school employee or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what data and features were accessed.

Subd. 5. **No access to student's password-protected software, Web site accounts, or applications; exceptions.** No school employee, or an agent thereof, may use a 1-to-1 device, or require a student to use a 1-to-1 device in their presence, in order to view or gain access to a student's password-protected software, Web site accounts or applications, except where:

(1) the school employee is a teacher;

(2) the student is enrolled in and participating in a class taught by the teacher; and

(3) the viewing of the 1-to-1 device relates exclusively to an educational purpose.

Subd. 6. **Prohibited uses of student data.** No 1-to-1 device provider, or an agent thereof, may use any student data or personally identifiable student information stored on or retrieved from a 1-to-1 device to:

(1) inform, influence, or direct marketing or advertising efforts directed at a student, a student's parent or legal guardian, or a school employee, except pursuant to a valid opt-in agreement; or

(2) develop, in full or in part, a student profile for any commercial or other noneducational purpose.

Subd. 7. **Training required.** Notwithstanding any other provisions in this section, no school employee may supervise, direct, or participate in a 1-to-1 program, or access any 1-to-1 device or data thereupon, until the school employee has received adequate training to ensure the school employee's understanding and compliance with the provisions of this section.

Subd. 8. **No sharing of personally identifiable student information; exceptions.** No personally identifiable student information obtained or received from a 1-to-1 device by a school employee or 1-to-1 device provider may be sold, shared, or otherwise transferred to another person or entity, except:

(1) to another school employee who has satisfied the requirements of subdivision 7 and is accessing the information in furtherance of the employee's professional duties; or

(2) where a 1-to-1 device provider has been authorized to do so pursuant to an opt-in agreement under subdivision 9.

Subd. 9. **Opt-in agreements.** (a) For purposes of this section, a valid opt-in agreement shall identify, with specificity:

(1) the precise subset of personally identifiable student information on the 1-to-1 device to which the authority to access, analyze, and interact is being granted;

(2) the name of the school employee or 1-to-1 device provider to whom the authority to access, analyze, and interact with the personally identifiable student information on the 1-to-1 device is being granted;

(3) the educational purpose for which the school employee or 1-to-1 device provider is being granted the authority to access, analyze, and interact with the personally identifiable student information on the 1-to-1 device; and

(4) the individual student to whom the opt-in agreement applies.

(b) An opt-in agreement shall only be valid if it has been signed by:

(1) the student's parent or guardian, if the student is in elementary school;

(2) the student and the student's parent or legal guardian, if the student has advanced beyond elementary school but has not yet reached the age of majority; or

(3) the student alone, if the student has reached the age of majority.

(c) An opt-in agreement shall not be valid if it actually or effectively grants a 1-to-1 device provider:

(1) general authority to access a student's 1-to-1 device; or

(2) the authority to collect all the personally identifiable student information that is generated by or used in connection with a specific program or application.

(d) An opt-in agreement may be revoked at any time, upon written notice to an educational institution, by the person eligible to authorize an opt-in agreement pursuant to paragraph (b). Within 30 days of such a revocation, notice to any affected third parties shall be made by the educational institution.

(e) A 1-to-1 device provider that accesses, analyzes, or interacts with personally identifiable student information on a 1-to-1 device shall bear the burden of proving that it acted pursuant to a valid opt-in agreement.

(f) No 1-to-1 device program offered to an educational institution or its students may be conditioned upon the exclusive use of any software, application, Web site, or Internet-based service sold to or provided by the 1-to-1 device provider.

(g) No 1-to-1 device or related educational benefit may be withheld from, or punitive measure taken against, a student or the student's parent or legal guardian:

(1) based in whole or in part upon a decision not to sign, or to revoke, an opt-in agreement; or

(2) based in whole or in part upon a student's refusal to open, close, or maintain an e-mail or other electronic communications or social media account with a specific service provider.

(h) A 1-to-1 device provider shall violate paragraph (g), clause (1), if it conditions the offer, provision, or receipt of a 1-to-1 device upon a student's or the student's parent's or legal guardian's agreement to provide access to personally identifiable student information.

Subd. 10. **No sale, sharing, or transfer of personally identifiable student information; exception.** No school employee or 1-to-1 device provider, or an agent thereof, who receives or collects personally identifiable student information from a 1-to-1 device may share, sell or otherwise transfer such data to another person or entity unless, in the case of a 1-to-1 device provider, such information is sold as part of a sale or merger of the entirety of the 1-to-1 device provider's business. Any entity that purchases personally identifiable student information pursuant to subdivision 9, paragraph (c), shall be subject

to the same restrictions and obligations under this section as the 1-to-1 device provider from which the personally identifiable student information was obtained.

Subd. 11. **Direct access prohibited; exceptions.** No person or entity, other than an educational institution, school employee, or 1-to-1 device provider subject to the limitations set forth in this section, shall be provided direct access to review or interact with a 1-to-1 device and the data thereon, unless otherwise authorized to do so by law, pursuant to a judicial warrant, or upon the express permission of the student to whom the 1-to-1 device is issued.

Subd. 12. **Return of 1-to-1 device; erase data.** When a 1-to-1 device is permanently returned by a student, the educational institution or 1-to-1 device provider who provided it shall, without otherwise accessing the data on the 1-to-1 device, fully erase all the data stored on the device and return the device to its default factory settings.

Subd. 13. **Personally identifiable student data; general exceptions.** The provisions of this section that relate to the collection and use of personally identifiable student information shall not apply to personally identifiable student information collected by a 1-to-1 provider from a software program, Web site or application that was:

(1) not preloaded on the 1-to-1 device;

(2) not the target of a link that was preloaded on the 1-to-1 device; and

(3) not promoted, marketed, or advertised in connection with the issuance of the 1-to-1 device.

Sec. 5. **[125B.34] STUDENT'S PERSONAL ELECTRONIC DEVICES ON CAMPUS.**

(a) No school employee may access, or compel a student to produce, display, share, or provide access to data or other content input into, stored upon, or accessible from a student's personal technological device, even when the personal technological device is being carried or used in violation of an educational institution policy.

(b) Notwithstanding paragraph (a), a school employee may search a student's personal technological device if:

(1) the school employee has a reasonable suspicion that a student has violated or is violating an educational institution policy and the student's personal technological device contains evidence of the suspected violation. In such cases, the school employee may search the student's personal technological device if:

(i) the student's personal technological device is located on the property of the educational institution;

(ii) prior to searching a student's personal technological device, the school employee:

(A) documents the reasonable individualized suspicion giving rise to the need for the search; and

(B) notifies the student and the student's parent or legal guardian of the suspected violation and what data will be accessed in searching for evidence of the violation;

(iii) the search is strictly limited to finding evidence of the suspected policy violation; and

(iv) the school employee immediately ceases searching the student's personal technological device upon finding sufficient evidence of the suspected violation; or

(2) the school employee believes doing so is necessary in response to an imminent threat to life or safety. Within 72 hours of accessing a personal technological device in response to an imminent threat to life or safety, the school employee or law enforcement official who accessed the device shall provide the student whose device was accessed, the student's parent or legal guardian, and the educational institution a written description of the precise threat that prompted the access and what data was accessed.

(c) For purposes of a search under paragraph (b), clause (1), an educational institution, subject to any other relevant legal restrictions, may seize a student's personal technological device to prevent data deletion pending notification. In the case of a seizure under this paragraph, the prenotification seizure period must be no greater than 48 hours, and the personal technological device must be stored securely on educational institution property and not accessed during the prenotification seizure period.

(d) The school employee shall not copy, share, or transfer any data or information that is unrelated to the specific suspected violation that prompted a search of the student's personal technological device under paragraph (b), clause (1).

(e) Notwithstanding paragraph (b), clause (1), if a student is suspected of illegal conduct, no search of the student's personal technological device may occur unless a judicial warrant authorizing a law enforcement official to search the student's personal electronic device has been secured, even if the student is also suspected of a related or unrelated violation of an educational institution policy.

Sec. 6. **[125B.35] LIMITATIONS ON USE.**

Evidence or information obtained or collected in violation of sections 125B.30 to 125B.37 shall not be admissible in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing.

Sec. 7. **[125B.36] PENALTIES.**

(a) Any person or entity who violates sections 125B.30 to 125B.37 shall be subject to legal action for damages or equitable relief, to be brought by any other person claiming that a violation of sections 125B.30 to 125B.37 has injured that person or that person's reputation. A person so injured shall be entitled to actual damages, including mental pain and suffering endured on account of violation of the provisions of sections 125B.30 to 125B.37, and reasonable attorney fees and other costs of litigation.

(b) Any school employee who violates sections 125B.30 to 125B.37, or any implementing rule or regulation, may be subject to disciplinary proceedings and punishment. For school employees who are represented under the terms of a collective bargaining agreement, sections 125B.30 to 125B.37 prevail except where they conflict with the collective bargaining agreement, any memorandum of agreement or understanding signed pursuant to the collective bargaining agreement, or any recognized and established practice relative to the members of the bargaining unit.

Sec. 8. **[125B.37] SEVERABILITY.**

The provisions in sections 125B.30 to 125B.37 are severable. If any part or provision of sections 125B.30 to 125B.37, or the application of sections 125B.30 to 125B.37 to any person, entity, or circumstance, is held invalid, the remainder of sections 125B.30 to 125B.37, including the application of such part or provision to other persons, entities, or circumstances, shall not be affected by such holding and shall continue to have force and effect.

Sec. 9. **EFFECTIVE DATE.**

Sections 1 to 8 are effective January 1, 2017."

Amend the title accordingly