SENATE
STATE OF MINNESOTA
NINETIETH SESSION

S.F. No. 1961

(SENATE AUTHORS: PRATT, Limmer, Chamberlain, Dibble and Kent)

DATE	D-PG	OFFICIAL STATUS
03/08/2017	1191	Introduction and first reading Referred to E-12 Policy
03/05/2018		Chief author stricken Abeler
	6280	Chief author added Pratt
03/08/2018		Comm report: To pass as amended and re-refer to Judiciary and Public Safety Finance and Policy Author stricken Isaacson Author added Kent

A bill for an act

relating to education; creating the Student Data Privacy Act; providing penalties; amending Minnesota Statutes 2016, section 13.319, by adding a subdivision; proposing coding for new law in Minnesota Statutes, chapter 125B.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 2016, section 13.319, is amended by adding a subdivision to read:

Subd. 9. **Technological devices for students.** Sections 125B.30 to 125B.36 regulate some educational data on students maintained using a software application or obtained from certain technological devices.

Sec. 2. **[125B.30] CITATION.**

Sections 125B.30 to 125B.36 may be cited as the "Student Data Privacy Act."

Sec. 3. **[125B.31] DEFINITIONS.**

(a) For the purposes of sections 125B.30 to 125B.36 and consistent with section 13.32, the following terms have the meanings given them.

(b) "Aggregate data" means educational data under section 120B.11, 120B.35, or 127A.70, subdivision 2, paragraph (b), or other data an educational institution collects and reports at the group, cohort, or institutional level that contains no personally identifiable student information.

(c) "De-identified data" means educational data on students in which personally identifiable student information is removed or obscured to prevent the unintended disclosure of a student's identity or other personally identifiable student information.

(d) "Education research" means the systematic gathering and study of empirical, personally identifiable student information to acquire knowledge, answer questions, identify trends, or improve educational instruction or effectiveness on behalf of an educational institution.

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

(f) "Educational institution" means:

(1) a nonpublic school under section 123B.41, subdivision 9, excluding a home school;

(2) an early learning and care program participating in the quality rating and improvement system under section 124D.142 or a prekindergarten program under section 124D.151;

(3) a public elementary, kindergarten, middle, secondary, or vocational center school under section 120A.05, subdivision 9, 10a, 11, 13, or 17;

(4) a school district under section 120A.05, subdivision 10;

(5) a charter school under chapter 124E; or

(6) a state or local educational agency authorized to direct or control an educational institution under clauses (1) to (5).

(g) "Eligible student" means a student who is age 18 or older or who is attending a postsecondary institution.

(h) "Law enforcement official" means an officer or employee of a state agency or a political subdivision, or an agent of the agency or subdivision, authorized by law or an agreement with an educational institution to investigate or conduct an official inquiry into a student's possible law violation, to arrest a student, or to prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from a student's alleged law violation. A law enforcement official is not a school employee under paragraph (p).

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

(j) "One-to-one device" means a technological device an educational institution provides to a student under a one-to-one program.

(k) "One-to-one device provider" means a person or entity under contract or other agreement to provide a one-to-one device to a student or educational institution under a one-to-one program, and includes any business or nonprofit entity directly or indirectly owned by the entity providing the one-to-one device.

(l) "One-to-one program" means a program under which an educational institution provides a technological device to a student for overnight or at-home use.

(m) "Opt-in agreement" means a verifiable, written or electronically generated, signed agreement under which a parent, guardian, or eligible student voluntarily grants a school employee, SIS provider, or one-to-one device provider limited access to personally identifiable student information.

(n) "Parent" means a parent, guardian, or other person having legal custody of a child as defined in section 120A.22, subdivision 3.

(o) "Personally identifiable student information" means educational data on a student under section 13.32 or Code of Federal Regulations, title 34, section 99.3, when it appears with direct identifiers, including but not limited to the student's or parent's name, date of birth, student identification number, address, telephone number, e-mail address, biometric information, Social Security number, or other information that would allow the student to be discovered.

(p) "School employee" means an individual employed and compensated by an educational institution who provides education-related services at a physical location owned or leased by an educational institution or online under section 124D.095 at the direction of an educational institution.

(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 child subject to the compulsory attendance requirements under section 120A.22 enrolled full time or part time in an educational institution.

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

(t) "Technological device" means any computer, cellular phone, smartphone, digital camera, video camera, audio recording device, or other electronic device used to create, store, or transmit information as electronic data.

Sec. 4. **[125B.32] STUDENT INFORMATION SYSTEMS.**

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

(1) establish, implement, and maintain appropriate security measures, consistent with department guidelines and current best practices, to protect educational data and personally identifiable student information the SIS provider creates, sends, receives, stores, or transmits to operate the SIS;

(2) affirm that all data stored on the SIS is the property of the educational institution and is not the property of the SIS provider and contain the notice requirements in section 13.05, subdivision 11, when the contract is with a public educational institution;

(3) establish and implement policies and procedures to respond to data breaches involving an unauthorized person or entity acquiring or accessing personally identifiable student information on the SIS that, at a minimum:

(i) require the SIS provider to provide notice to all affected parties, including parents, guardians, eligible students, teachers, and school administrators, within 14 days after discovering the breach by United States mail or e-mail, or if the SIS provider has insufficient or out-of-date contact information for ten or more individuals, the SIS provider must provide substitute individual notice by posting the notice on its Web site for at least 90 days:

(A) briefly describing the breach, including a description of the educational data the unauthorized person or entity acquired or accessed, or is reasonably believed to have acquired or accessed;

(B) informing the affected parties about the educational data the SIS provider maintains on the student;

(C) describing the steps affected individuals should take to protect themselves from potential harm;

(D) briefly describing what the SIS provider is doing to investigate the breach, mitigate the harm, and prevent further breaches; and

(E) providing contact information for the SIS provider so affected individuals may obtain more information; and

(ii) satisfy all other applicable notice requirements;

(4) permanently delete all data stored on the SIS and destroy all nondigital records containing any educational data retrieved from the SIS within 30 days after the educational institution terminates the SIS provider's contract, except where:

(i) the SIS provider and the person authorized to sign an opt-in agreement under subdivision 2 direct the SIS provider to retain educational data, specifically identified data, or nondigital records for a student's benefit; or

(ii) before deleting the stored data, the educational institution directs the terminated SIS provider to transfer data stored on the SIS to another designated SIS provider at the educational institution's expense; and

(5) comply with all obligations and restrictions applicable to SIS providers in sections 125B.30 to 125B.36.

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

(1) analyzing, interacting with, sharing, or transferring any educational data or personally identifiable student information the educational institution transmits to the SIS except as allowed by the opt-in agreement in subdivision 2, paragraph (b);

(2) selling any educational data or personally identifiable student information stored on or retrieved from the SIS unless the SIS is sold as part of a sale or merger of the SIS provider's business and the new purchaser or controlling person or entity is subject to sections 125B.30 to 125B.36 and any existing contract or agreement binding successors and assigns;

(3) using any educational data or personally identifiable student information stored on or retrieved from the SIS for marketing or advertising directed at a student, parent, guardian, or school employee, except under an opt-in agreement signed under subdivision 2; and

(4) using any educational data or personally identifiable student information stored on or retrieved from the SIS to develop a profile of a student or group of students for a commercial or noneducational purpose.

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

(1) the educational data on a student contained in the SIS, including student attendance and disciplinary records, that the SIS provider may access, analyze, interact with, share, or transfer;

(2) the SIS provider authorized to access, analyze, interact with, share, or transfer educational data in the SIS and what the SIS provider is authorized to do with that educational data, including allowing:

(i) the SIS provider to analyze or interact with the educational data or personally identifiable student information to meet a contractual obligation to the educational institution to analyze or interact with the data for an educational purpose;

(ii) the educational institution to determine, and document in writing, that sharing specific educational data or personally identifiable student information is needed to safeguard students' health or safety;

(iii) the SIS provider to de-identify or aggregate educational data or personally identifiable student information at the request of the educational institution to:

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

(B) undertake education research; or

(iv) the SIS provider to access the data to test and improve the value and performance of the SIS for the educational institution and the SIS provider permanently deletes any copied data and any data analysis within 60 days after creating the copy or the data analysis;

(3) the educational purpose for the SIS to access the educational data; and

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

(b) The opt-in agreement is valid only if signed by:

(1) a parent or guardian, if the student is under age 18; or

(2) an eligible student.

(c) An opt-in agreement signed under this subdivision may include a provision to authorize an SIS provider to share or transfer educational data if:

(1) the purpose of the transfer is to benefit:

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

(ii) the student's education;

(2) the opt-in agreement specifically identifies:

(i) the educational data to be shared or transferred;

(ii) when and with whom the educational data will be shared or transferred; and

(iii) the anticipated benefits to the educational institution or student; and

(3) the SIS provider includes a record of the educational data to be shared or transferred prior to the opt-in agreement being signed.

(d) Any person or entity that accesses or possesses any educational data or personally identifiable student information from an SIS provider is subject to the same restrictions and obligations under this section as the SIS provider providing the educational data or personally identifiable student information to that person or entity.

(e) An opt-in agreement is invalid if it grants general authority to access, analyze, interact with, share, or transfer educational data or personally identifiable student information in an SIS.

(f) Except as authorized in this section, no SIS provider, school employee, or other person or entity that receives educational data or personally identifiable student information, directly or indirectly, from an SIS under an opt-in agreement may share, sell, or otherwise transfer the information to another person or entity consistent with the requirements in section 13.05, subdivision 11.

(g) A parent, guardian, or eligible student under paragraph (b) may revoke the agreement at any time by transmitting written notice to the educational institution. The educational institution must notify the SIS provider within 14 days after receiving the revocation notice.

(h) An SIS provider that accesses, analyzes, interacts with, shares, or transfers educational data or personally identifiable student information to another person or entity must show it acted under an opt-in agreement signed under this subdivision.

(i) An educational institution must not withhold an educational benefit from or penalize a student, parent, or guardian who does not sign or who revokes an opt-in agreement.

(j) An opt-in agreement must be renewed at least annually.

Subd. 3. **School employees.** (a) Subject to written authority from the educational institution, and for purposes of this subdivision, school employees may access and interact with educational data and personally identifiable student information on an SIS to perform their professional duties. To access or interact with educational data or personally identifiable student information on an SIS, a school employee must receive periodic training to ensure the school employee understands and can comply with the requirements of this section.

(b) A school employee may transfer educational data to the employing educational institution or another trained school employee only if:

(1) the school employee has completed periodic and at least annual training in data practices under this subdivision and section 125B.35, and for compliance with section 121A.065 and the federal Family Educational Rights and Privacy Act (FERPA);

(2) the school employee is a teacher transferring educational data to a district-approved software application for classroom record keeping or management purposes;

(3) any third party with access to the software application is expressly prohibited from reviewing or interacting with the transferred data; and

(4) the teacher deletes the data transferred to the software application within 30 days after the teacher no longer uses the data for classroom record keeping or management purposes.

Subd. 4. **Parent or guardian access to educational data.** (a) Consistent with state and federal data practices law as applied to this subdivision, a parent, guardian, or eligible student, upon transmitting a written request to an educational institution, may inspect and review the student's educational data and personally identifiable student information stored on an SIS. An educational institution must give parents, guardians, and eligible students an opportunity to correct or remove inaccurate educational data.

(b) The right of a parent or guardian to review a minor student's educational record or other personally identifiable student information does not apply where:

(1) the minor student supplied health information to the educational institution; and

(2) the responsible authority determines that withholding the data is in the minor student's best interest under sections 13.02, subdivision 8, and 144.29.

(c) When a student is age 18 or older, the rights of a parent or guardian under this subdivision terminate and the eligible student assumes those rights.

(d) An educational institution must:

(1) review and respond to requests made under this subdivision within five days after receiving the request; and

(2) provide a parent, guardian, or eligible student a hearing if the educational institution denies the parent, guardian, or eligible student's request to correct or remove inaccurate information and, if the school does not amend the record after the hearing, allow the parent, guardian, or eligible student to insert a statement in the record contesting the information.

Subd. 5. **Requirements for deleting data in an SIS.** An educational institution must permanently delete all educational data and personally identifiable student information on a student stored in an SIS within one school year after a student graduates, withdraws, or is expelled from the educational institution. This provision does 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 a postsecondary institution for admission to the institution or by a potential employer;

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

(4) de-identified educational data retained at the request of the educational institution for education research or analysis; and

(5) educational data or personally identifiable student information required by law or a judicial order or warrant to be retained.

Subd. 6. **Requirements for deleting physical or digital copies of educational data.** Within 180 days of receiving notice under subdivision 7, an SIS provider or other third party possessing or controlling educational data or other personally identifiable student information related to a student's graduation, withdrawal, or expulsion from an educational institution must permanently destroy or delete all physical or digital copies of the data. This provision does not apply to:

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

(2) aggregated or de-identified educational data obtained for education research;

(3) educational data or personally identifiable student information required by law or a judicial order or warrant to be retained; and

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

(i) the person authorized to sign a valid opt-in agreement under subdivision 2, paragraph (b), requests the data be retained; and

(ii) the SIS provider and educational institution agree to retain the data.

Subd. 7. **Notice to SIS provider and third parties.** Within 90 days, an educational institution must notify its SIS provider when a student graduates, withdraws, or is expelled

from school, and the SIS provider then must immediately notify any third party it allowed to access that student's education record or personally identifiable student information of the student's changed status.

Subd. 8. **Access under law, judicial warrant, or audit.** Except as provided under this section, no person or entity, other than an educational institution, school employee, or SIS provider shall access or interact with an SIS or SIS data unless authorized by law, under a judicial warrant, or as part of an educational institution audit.

Subd. 9. **Directory information permitted.** Consistent with section 13.32, subdivision 5, an educational institution may provide directory information to a vendor providing photographs, class rings, yearbooks or student publications, memorabilia, or other similar goods or services to students if the vendor agrees in writing:

(1) not to sell or transfer the data to any other person or entity;

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

(3) to destroy the data after using the data for its intended purpose.

Subd. 10. **Interaction with other law.** Nothing in this section supersedes or otherwise changes the classification of data in chapter 13, or limits any law that enhances privacy protections to students or otherwise restricts access to students' educational records or personally identifiable student information.

Sec. 5. **[125B.33] ONE-TO-ONE PROGRAMS; ACCESS TO DATA.**

Subdivision 1. **General rule; contract.** (a) When an educational institution or one-to-one device provider provides a student with a technological device in a one-to-one program, no school employee or one-to-one device provider, or their agent, may access or track the student's one-to-one device, activity, or data, either remotely or in person, except as consistent with this section.

(b) Any contract or other agreement between an educational institution and a one-to-one device provider for a one-to-one provider to provide one-to-one devices for the benefit of the educational institution shall:

(1) affirm that the student's educational data on the devices are the property of the student and the educational institution and not the property of the one-to-one device provider;

(2) contain the notice requirements in section 13.05, subdivision 11, when the contract is with a public educational institution; and

(3) prohibit the sale, sharing, or use of educational data or personally identifiable student information in violation of sections 125B.30 to 125B.36.

Subd. 2. **Exceptions.** No school employee or one-to-one device provider, or their agent, may access any data such as the browser, keystroke, or location history the student inputs into, stores upon, or sends or receives on the student's one-to-one device, nor may the school employee or one-to-one device provider analyze, interact with, share, or transfer such data except when:

(1) the data is de-identified or aggregate data;

(2) the school employee accessing the data:

(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 another person or entity to use the information for any other purpose;

(3) a school employee or one-to-one device provider, or their agent, is authorized to access the educational data under an opt-in agreement under subdivision 9;

(4) a school employee reasonably suspects the student violated or is violating a law or a school rule and data on the one-to-one device contains evidence of the suspected violation, subject to the following limitations:

(i) before searching a student's one-to-one device, the school employee must document the basis for the reasonable 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, consistent with other law, may seize a student's one-to-one device to prevent the student from deleting data pending parent notification if:

(A) the prenotification seizure period does not exceed 48 hours; and

(B) the school employee securely stores the one-to-one device on educational institution property and does not access it during the prenotification seizure period;

(ii) searches of a student's one-to-one device are strictly limited to finding evidence of the suspected violation and must immediately cease when the school employee finds evidence of the suspected violation. A school employee who copies, shares, or transfers any data or any other student information unrelated to the suspected violation violates this item; and

(iii) when a student is suspected of illegal conduct, no school employee or law enforcement official may search the one-to-one device without first securing a judicial warrant under clause (5) even if the student is also suspected of violating another law or school rule;

(5) a school employee or law enforcement official reasonably suspects the student engaged in or is engaging in illegal conduct, reasonably suspects data on the student's one-to-one device contain evidence of the suspected illegal conduct, and secures a judicial warrant to search the device;

(6) doing so is needed to update or upgrade a one-to-one device's software, or protect the device from cyber threats, and access is limited to that purpose;

(7) doing so is needed to respond to an imminent threat to life or safety and access is limited to that purpose. Within 72 hours of accessing a student's data on a one-to-one device under this clause, the school employee or law enforcement official who accessed the one-to-one device must provide a written description of the precise threat allowing access and the data accessed to the educational institution and the eligible student, parent, or guardian; or

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

(i) is accessible to the general public; or

(ii) is accessible to a specific school employee granted written permission by the eligible student, parent, or guardian to view the content.

Subd. 3. **Use of location tracking technology.** No law enforcement official, school employee, or one-to-one device provider, or their agent, may use a student's one-to-one device's location tracking technology to track a one-to-one device's real-time or historical location unless:

(1) such use is ordered under a judicial warrant;

(2) a parent, guardian, or the student to whom the one-to-one device was provided notifies a school employee or law enforcement official that the one-to-one device is missing or stolen; or

(3) doing so is needed to respond to an imminent threat to life or safety and access is limited to that purpose. Within 72 hours of accessing the location tracking technology of a student's one-to-one device, the school employee or law enforcement official who accessed the one-to-one device must provide a written description of the precise threat allowing

access and the data and features accessed to the educational institution and the eligible student, parent, or guardian.

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

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

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

(3) doing so is needed to respond to an imminent threat to life or safety and access is limited to that purpose. Within 72 hours of accessing the audio or video receiving, transmitting, or recording functions of a student's one-to-one device, the school employee or law enforcement official who accessed the one-to-one device must provide a written description of the precise threat allowing access and the data and features accessed to the educational institution and the eligible student, parent, or guardian.

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

(1) the school employee is a teacher;

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

(3) viewing of the one-to-one device serves an educational purpose in that class.

Subd. 6. **Prohibited uses of educational data.** No one-to-one device provider or its agent may use any educational data stored on or retrieved from a one-to-one device in a manner inconsistent with an opt-in agreement under subdivision 9 or to:

(1) market or provide advertising directed at a student, parent, guardian, or school employee, except under an opt-in agreement signed under subdivision 9; or

(2) develop a student profile for any commercial or other noneducational purpose.

Subd. 7. **Training required.** Notwithstanding other provisions in this section, to supervise, direct, or participate in a one-to-one program, or to access any one-to-one device or its data, a school employee must receive periodic and at least annual training under section 125B.35 to ensure the school employee understands and complies with the provisions of

this section, section 121A.065, and the federal Family Educational Rights and Privacy Act (FERPA).

Subd. 8. **No sharing of personally identifiable student information; exceptions.** No school employee or one-to-one device provider that obtains or receives educational data from a one-to-one device may transfer the information except:

(1) to another trained school employee and the employee accesses the information as part of the employee's professional duties; or

(2) where a one-to-one device provider is authorized access under an opt-in agreement signed under subdivision 9.

Subd. 9. **Opt-in agreements.** (a) For purposes of this section, and to the extent applicable, a valid opt-in agreement must comply with the requirements in section 125B.32, subdivision 2, and must specifically identify:

(1) the educational data on the one-to-one device to which access is granted;

(2) the school employee or one-to-one device provider authorized to access, analyze, and interact with the educational data on the one-to-one device;

(3) the educational purpose for which the school employee or one-to-one device provider will access, analyze, and interact with the educational data on the one-to-one device; and

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

(b) The opt-in agreement is valid only if signed by:

(1) a parent or guardian, if the student is under age 18; or

(2) an eligible student.

(c) An opt-in agreement is invalid if it grants a one-to-one device provider:

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

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

(d) A parent, guardian, or eligible student under paragraph (b) may revoke an opt-in agreement at any time by transmitting written notice to an educational institution. An educational institution must notify all affected parties within 14 days after receiving the revocation notice.

(e) A one-to-one device provider that accesses, analyzes, or interacts with educational data or personally identifiable student information on a one-to-one device must show it acted under an opt-in agreement signed under this subdivision.

(f) An educational institution must not withhold a one-to-one device or a related educational benefit, or punish a student, parent, or guardian based upon:

(1) a decision by an eligible student, parent, or guardian to not sign, or to revoke, an opt-in agreement; or

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

(g) A one-to-one device provider violates paragraph (f), clause (1), if it requires an eligible student, parent, or guardian to agree to give the provider access to personally identifiable student information as a condition of receiving access to the one-to-one device.

(h) An opt-in agreement must be renewed at least annually.

Subd. 10. **No sale, sharing, or transfer of personally identifiable student information; exception.** No school employee or one-to-one device provider, or their agent, who receives or collects educational data or personally identifiable student information from a one-to-one device may share, sell, or otherwise transfer such data to another person or entity unless, in the case of a one-to-one device provider, the information is sold as part of a sale or merger of the one-to-one device provider's business. Any entity buying educational data or personally identifiable student information is subject to the same restrictions and obligations under this section as the one-to-one device provider that acquired or sold the educational data or personally identifiable student information.

Subd. 11. **Direct access prohibited; exceptions.** Only a student, student's parent or guardian, educational institution, school employee, or one-to-one device provider subject to the limitations of this section may access, review, or interact with a one-to-one device and its data, unless access is otherwise authorized under law, by a judicial warrant, or with the express permission of the parent, guardian, or eligible student to whom the one-to-one device is issued.

Subd. 12. **Return of one-to-one device; data deletion.** When a student permanently returns a one-to-one device to the educational institution or to the one-to-one device provider who provided it, the educational institution or one-to-one device provider must permanently delete all data stored on the one-to-one device without otherwise accessing the data on the

one-to-one device and must return the one-to-one device to its default factory settings within 180 days of receiving the one-to-one device.

Subd. 13. **Personally identifiable educational data; general exceptions.** The provisions of this section on collecting and using educational data or personally identifiable student information do not apply to a student's information collected by a software program, Web site, or application that is incidental to the use of that software program, Web site, or application that was not:

(1) preloaded on the one-to-one device unless approved by the district for educational purposes;

(2) the target of a link preloaded on the one-to-one device; and

(3) promoted, marketed, or advertised in connection with issuing the one-to-one device.

Sec. 6. **[125B.34] LIMITATIONS ON USE.**

Evidence or information obtained or collected in violation of sections 125B.30 to 125B.36 is inadmissible in any civil or criminal trial or legal proceeding, student disciplinary action, or administrative hearing.

Sec. 7. **[125B.35] ANNUAL TRAINING REQUIRED TO PROTECT EDUCATIONAL DATA.**

Subdivision 1. **Training required.** Every school district must conduct annual training sessions for administrative staff, IT directors, teachers, and any other individual with access to educational data to ensure compliance with the federal Family Educational Rights and Privacy Act (FERPA) and to prevent any unauthorized access, disclosure, or misuse of educational data, as defined in United States Code, title 20, section 1232g, and Code of Federal Regulations, title 34, part 99.

Subd. 2. **Best practices.** Training sessions under subdivision 1 shall include discussion and materials on FERPA best practices, which may include but are not limited to:

(1) maintaining awareness of relevant data privacy laws;

(2) maintaining awareness of all online educational services used in the district;

(3) maintaining policies to evaluate and approve online educational services;

(4) using written contracts governing the use of educational data;

(5) maintaining transparency with students and their parents or legal guardians; and

(6) considering when parental consent may be appropriate or required under applicable law.

Sec. 8. **[125B.36] PENALTIES.**

(a) Any person or entity that violates sections 125B.30 to 125B.36 is subject to legal action for damages or equitable relief brought by a person claiming injury to the person or the person's reputation. A prevailing plaintiff may be awarded equitable relief, special and general damages, and reasonable attorney fees and costs.

(b) Nothing in sections 125B.30 to 125B.36 limits the civil or criminal liability of a person or entity who violates the federal Family Educational Rights and Privacy Act (FERPA), as defined in United States Code, title 20, section 1232g, and Code of Federal Regulations, title 34, part 99, or under the Data Practices Act, section 13.08 or 13.09.

Sec. 9. **EFFECTIVE DATE.**

Sections 1 to 8 are effective January 1, 2018.