

File Number: H.F. 1507 **Date:** February 27, 2018
Version: Delete Everything Amendment (H1507DE3)

Authors: Lucero

Subject: Student Data Privacy

Analyst: Nathan Hopkins (651-296-5056)

This publication can be made available in alternative formats upon request. Please call 651-296-6753 (voice); or the Minnesota State Relay Service at 1-800-627-3529 (TTY) for assistance. Summaries are also available on our website at: www.house.mn/hrd/.

Overview

This bill creates new protections for student data privacy within the Minnesota Government Data Practices Act's existing educational data section. The bill expands privacy protections for student data that is maintained by "technology providers," which are nongovernmental entities that contract with schools. The bill also gives students new privacy rights in technological devices (laptops, tablets, etc.) that a school issues to students for their individual use. Finally, the bill requires schools to create audit trails that show who has accessed a student's electronic records, and provide annual privacy training for employees with access to student data.

The main provisions of the bill would apply to both public and private K-12 schools, but not to public postsecondary institutions. All sections of the bill are effective January 1, 2019.

Section

- 1** **Definitions.** Amends the definitions subdivision of the Government Data Practices Act's educational data section.
- The "educational data" definition is amended to clarify that student data maintained by technology providers—or other government contractors—is "educational data."
 - A definition for "parent" is added.
 - "School-issued device" is any technological device that a school issues to a student for the student's dedicated personal use.

Section

- “Technology provider” is a person (includes individuals, business entities, and other organizations) who: (1) contracts with a school to provide technological devices for student use or provide access to software or an online application; and (2) has access to educational data pursuant or incidental to that contract.

2 **Audit trail required for electronic student data.** Requires a school to establish procedures that secure electronic student data and permit only authorized individuals to access the data. The school must also maintain a log-of-use that records any instance when an individual accesses electronic student data.

3 **Training required.** Requires a school to provide annual training on student privacy law for school personnel with access to student data.

4 **Technology providers.** This section imposes new requirements on technology providers and on schools that contract with technology providers.

- a) Makes explicit that technology providers are subject to the Government Data Practices Act (GDPA) under the privatization subdivision of section 13.05 (sometimes referred to as the “Timberjay” subdivision).
- b) Provides that all educational data which a technology provider creates, receives, or maintains as part of its contract with a school do not become the technology provider’s property.
- c) Makes technology providers subject to the GDPA’s existing data breach notification law at section 13.055.
- d) Requires a technology provider to destroy or return to the school all educational data created, received, or maintained under its contract.
- e) Prohibits a technology provider from selling, sharing, or disseminating education data except as part of a valid delegation or assignment of its contract with the school (e.g., if the technology provider’s business is sold to another company).
- f) Prohibits a technology provider from using educational data for any commercial purpose, such as advertising.
- g) Requires a technology provider to establish procedures that secure educational data and permit only authorized individuals to access the data. The technology provider must also maintain a log-of-use that records any instance when an individual accesses student data.
- h) Requires a school to annually notify parents and students of its technology provider contracts. Specifies content of the notice.
- i) Requires a school to allow students and parents to inspect technology provider contracts and to opt out of programs that involve data-sharing with a technology provider.
- j) Prohibits a school from penalizing a student who opts out of a technology provider program. Requires an opt-out to be renewed at least annually.

5 **School-issued devices.** This section gives students privacy rights in school-issued devices.

Section

- a) Subject to the exceptions in paragraph (b), prohibits a government entity (schools, law enforcement, etc.) or technology provider from location-tracking a device; accessing the device's camera or microphone; or monitoring student interaction with the device.
- b) Allows a government entity or technology provider to engage in activities prohibited under paragraph (a) if: it is done for an educational purpose and the student consents; it is permitted by a judicial warrant; the device is missing or stolen; or the activity is necessary to respond to an imminent threat to life or safety.
- c) If a government entity or technology provider monitors the device due to an imminent threat to life or safety, it must provide notice and an explanation of the rationale for its action to the student or parent. This notice is not required if it would also pose a threat to life or safety.

6 **Application to nonpublic schools; exemption.** Makes the provisions of sections 3, 4, and 5 apply to private K-12 schools. Private schools are not normally subject to the Government Data Practices Act. Exempts public postsecondary institutions from sections 3, 4, and 5.