SPONSOR: Sen. Sokola & Rep. Jaques & Rep. Ramone
Sens. Henry, Marshall, Peterson; Reps. Briggs King, Keeley, Lynn, Matthews, Miro, Osienski, K. Williams

DELAWARE STATE SENATE
148th GENERAL ASSEMBLY

SENATE BILL NO. 79

AN ACT TO AMEND TITLE 14 OF THE DELAWARE CODE RELATING TO EDUCATIONAL DATA GOVERNANCE.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE:

Section 1. Amend § 4111, Title 14 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underline as follows:

§ 4111. ~~Disclosure~~ Privacy, accessibility, and transparency of ~~pupils' school~~ student records.

(a) *Definitions*. The following words, terms and phrases, when used in this section, shall have the meaning ascribed to them except where the context clearly indicates a different meaning:

(1) "Aggregate student data" means data that is not personally identifiable and that is collected or reported at the group, cohort, or institutional level.

(2) "De-identified data" means a student data set that cannot reasonably be used to identify, contact, single out, or infer information about a student or device used by a student.

(3) "Department" means the Delaware Department of Education.

(4) "Education record" means an education record as defined in FERPA, the Individuals with Disabilities Education Act, § 1400 of Title 20 of the United States Code and implementing regulations, and other applicable state and federal privacy and confidentiality laws.

(5) "Eligible student" means a student who has reached 18 years of age or is attending an institution of postsecondary education.

(6) "FERPA" means the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and its implementing regulations, 34 C.F.R. part 99.3, as amended.

(7) "Geolocation data" means information that is, in whole or part, generated by, derived from, or obtained by the operation of an electronic device that can be used to identify the past, present, or future location of an electronic device, an individual, or both.

(8) "Internet" means, collectively, the myriad of computer and telecommunications facilities, including

equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

(9) "Internet service" means any service, system, website, application, or program, or portion thereof, including mobile applications and cloud computing services, which accesses the Internet or provides a user with access to the Internet.

(10) "K-12 school purposes" means purposes that customarily take place at the direction of a school, teacher, or school district or aid in the administration of school activities, including, but not limited to, instruction in the classroom or at home, administrative activities, preparing for postsecondary education or employment opportunities, and collaboration between students, school personnel, or parents, or are for the use and benefit of the school.

(11) "Law enforcement entity" means any government agency or any subunit thereof which performs the administration of criminal justice pursuant to statute or executive order, and which allocates a substantial part of its annual budget to the administration of criminal justice, including but not limited to the Delaware State Police, all law-enforcement agencies and police departments of any political subdivision of this State, the Department of Correction, and the Department of Justice.

(12) "Online contact information" means an e-mail address or any other substantially similar identifier that permits direct contact with an individual online, including but not limited to an instant messaging user identifier, a voice over internet protocol (VOIP) identifier, or a video chat user identifier.

(13) "Operator" means any person other than the Department, school districts, or schools, to the extent that the person:

a. Operates an Internet service with actual knowledge that Internet service is used for K-12 school purposes and was designed and marketed for K-12 school purposes; and

b. Collects, maintains, or uses student data in a digital or electronic format.

(14) "Provisional student data" means new student data proposed for inclusion in the state data system.

(15) "School" means any public or private school in the State providing educational instruction in one or more grades from kindergarten through grade 12.

(16) "Secretary" means the Secretary of the Department.

(17) "State-assigned student identifier" means the unique student identifier assigned by the State to each student that shall not be and shall not include the social security number of a student in whole or in part.

(18) "State data system" means a Department state-wide longitudinal data system which allows for the storage, description, management, and reporting of discrete data elements and bodies of information over time.

(19) "Student" means any individual attending a school in the State.

(20) "Student data" means any information regarding a student that meets any of the following:

a. Data descriptive of a student in any media or format, including:

i. Student personally identifiable information;

ii. State, local, school, or teacher administered assessment results, including participation information;

iii. Transcript information including but not limited to courses taken and completed, course grades and grade point average, credits earned, degree, diploma, credential attainment, or other school exit information;

iv. Attendance and mobility information between and within local school systems in the State;

v. The student's race, ethnicity, gender, or gender identity;

vi. Program participation information required by state or federal law;

vii. Disability status;

viii. Socioeconomic information;

ix. Food purchases; or

x. E-mails, text messages, instant messages, documents, search activity, photos, voice recordings; or

b. Such information that:

i. Is created or provided by a student, or the student's parent or legal guardian, to an employee or agent of the school district, charter school, or the Department;

ii. Is created or provided by a student, or the student's parent or legal guardian, to an operator in the course of the student's or parent's or legal guardian's use of the operator's Internet service for K-12 school purposes;

ii. Is created or provided by an employee or agent of the school district or school, to an

operator; or

iii. Is gathered by an operator through the operation of an operator's Internet service for K-12 school purposes.

(21) "Student personally identifiable information" means any information about a student that, individually or in combination with other information, can be used to distinguish or trace the identity of the student, or information that is linked to information that can be used to distinguish or trace the identity of the student, including the student's name (in whole or in part), signature, physical characteristics or description, residential, school, or other physical address, telephone number, online contact information, social security number, passport number, student identification number, driver's license number, state identification card number, alien registration number, insurance policy number, education history, employment history, bank account number, credit card number, debit card number, or any other financial information, geolocation data, DNA or other genetic material, medical information, or health insurance information, except that it does not include information that is publicly available that is lawfully made available to the general public from federal, state, or local government records.

(22) "Targeted advertising" means presenting advertisements to a student, or a student's parent or legal guardian, where the advertisement is selected based on information obtained or inferred from that student's online behavior, usage of applications, or student data. "Targeted advertising" does not include advertising to a student at an online location based upon that student's current visit to that location without collection and retention of a student's online activities over time.

(b) *Confidentiality of education records*. ~~Educational~~ Education records of students in all ~~public and private~~ schools ~~in this State~~ are deemed to be confidential. ~~Educational~~ Education records may be released, and student personally identifiable information contained therein disclosed, only in accordance with ~~rules and regulations of the Department of Education~~ the provisions of this section and other applicable state and federal law. ~~Such rules and regulations shall authorize the release of educational records upon written consent and shall establish the other terms and conditions on which educational records may and must be released.~~

(c) *Privacy and security of student data; Department responsibilities*. The Department shall promulgate rules and regulations relating to the privacy and protection of student data, and shall be responsible for ensuring compliance with this section and with other state and federal data privacy and security laws by the Department,

school districts, and schools, including by doing the following:

(1) Establishing Department-wide policies necessary to assure that the use of technologies sustains, enhances, and does not erode privacy protections relating to the use, collection, and disclosure of student data;

(2) Maintaining and accessing all records, reports, audits, reviews, documents, papers, recommendations, and other materials available to the Department that relate to programs and operations with respect to the responsibilities of the Department under this section;

(3) Ensuring that student data contained in the state data system is handled in full compliance with this section, FERPA, and other state and federal data privacy and security laws;

(4) Evaluating legislative and regulatory proposals involving use, collection, and disclosure of student data by the Department;

(5) Conducting a privacy impact assessment on legislative proposals, regulations, and program initiatives of the Department, including the type of personal information collected and the number of students affected;

(6) Making such investigations and reports relating to the administration of the programs and operations of the Department as are necessary or desirable;

(7) Coordinating with the Department of Justice and other legal entities as necessary to ensure that state programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner;

(8) Preparing an annual report to the General Assembly on activities of the Department that affect privacy, including complaints of privacy violations, internal controls, and other matters;

(9) Working with the Attorney General and other officials in engaging with stakeholders about the quality, usefulness, openness, and privacy of data;

(10) In matters relating to compliance with federal laws, referring the matter to the appropriate federal agency and cooperate with any investigations by such federal agency

(11) Establishing and operating a Department-wide Privacy Incident Response Program to ensure that incidents involving Department data are properly reported, investigated, and mitigated, as appropriate;

(12) Establishing a model process and policy for parents and eligible students to file complaints of privacy violations or inability to access their children's or their education records against the school district or

school; and

(13) Providing training, guidance, technical assistance, and outreach to build a culture of privacy protection, data security, and data practice transparency to students, parents, and the public among all state and local governmental education entities that collect, maintain, use, or share student data.

(d) *State data system and student personally identifiable information; Department responsibilities*. The Department shall:

(1) Create, publish, and make publicly available a data inventory and dictionary or index of data elements with definitions of student personally identifiable information fields in the state data system to include, but not be limited to:

a. Any student personally identifiable information required to be reported by state and federal education mandates;

b. Any student personally identifiable information which is included or has been proposed for inclusion in the state data system with a statement regarding the purpose or reason for the proposed collection; and

c. Any student data that the Department collects or maintains with no current identified purpose;

(2) Promulgate rules and regulations for the state data system to comply with this article and other applicable state and federal data privacy and security laws, including FERPA. Such rules and regulations shall include, at a minimum:

a. Restrictions on granting access to student data in the state data system, except to the following:

i. Students and their parents, as provided by the collecting school district or school;

ii. Authorized administrators, teachers, and other personnel of school districts or schools, and contractors or other authorized persons working on their behalf, that enroll students who are the subject of the data and who require such access to perform their assigned duties;

iii. Authorized staff of the Department, and contractors or other authorized persons working on behalf of the Department, who require such access to perform their assigned duties as authorized by law or defined by interagency or other data-sharing agreements; and

iv. Authorized staff of other State agencies as required or authorized by law, including contractors or other authorized persons working on behalf of a state agency that require such access to

perform their duties pursuant to an interagency agreement or other data-sharing agreement;

b. Prohibitions against publishing student data other than as specifically permitted herein; and

c. Consistent with applicable law, criteria for the approval of research and data requests from state and local agencies, the General Assembly, persons conducting research including on behalf of the Department, and the public that involve access to student personally identifiable information;

(3) Unless otherwise provided by law or approved by the Department, not transfer student personally identifiable information to any state, federal, or local agency or nongovernmental organization, except for disclosures incident to the following actions:

a. A student transferring to another school or school system in this State or out of state or a school or school system seeking help with locating a transferred student;

b. A student enrolling in a postsecondary institution or training program;

c. A student registering for or taking a state, national, or multistate assessment where such data is required to administer the assessment;

d. A student voluntarily participating in a program for which such a data transfer is a condition or requirement of participation;

e. The federal government requiring the transfer of student data for a student classified as a "migrant" for related federal program purposes;

f. A federal agency requiring student personally identifiable information to perform an audit, compliance review, or complaint investigation; or

g. An eligible student or student's parent or legal guardian requesting such transfer;

(4) Develop a detailed data security plan for the state data system that includes:

a. Guidelines for authorizing access to the state data system and to student personally identifiable information including guidelines for authentication of authorized access;

b. Privacy and security audits;

c. Plans for responding to security breaches, including notifications, remediations, and related procedures;

d. Data retention and disposal policies;

e. Data security training and policies including technical, physical, and administrative safeguards;

f. Standards regarding the minimum number of students or information that must be included in a data set in order for the data to be considered aggregated and, therefore, not student personally identifiable information subject to requirements in this article and in other federal and state data privacy laws;

g. A process for evaluating and updating as necessary the data security plan, at least on an annual basis, in order to identify and address any risks to the security of student personally identifiable information; and

h. Guidance for local boards of education to implement effective security practices that are consistent with those of the state data system;

(5) Ensure routine and ongoing compliance by the Department with FERPA, other relevant privacy laws and policies, and the privacy and security rules and regulations promulgated under the authority of this section, including the performance of compliance audits for the Department;

(6) Notify the Governor and the General Assembly annually of the following matters relating to the state data system:

a. New provisional student data proposed for inclusion in the state data system:

i. Any new provisional student data collection proposed by the Department shall become a provisional requirement to allow local boards of education and their local data system vendors the opportunity to meet the new requirement; and

ii. The Department shall announce any new provisional student data collection to the general public for a review and comment period of at least 60 days;

b. Changes to existing student personally identifiable information collections required for any reason, including changes to federal reporting requirements made by the United States Department of Education;

c. A list of any special approvals granted by the Department pursuant to paragraph (3)c. of subsection (d) of this section in the past year regarding the release of student personally identifiable information; and

d. The results of any and all privacy compliance and security audits completed in the past year. Notifications regarding privacy compliance and security audits shall not include any information that would itself pose a security threat to the state or local student information systems or to the secure transmission of

data between state and local systems by exposing vulnerabilities; and

(7) Promulgate rules and regulations to ensure the provision of at least annual notifications to eligible students and parents or guardians regarding student privacy rights under state and federal law.

(e) *Restrictions on reporting student data*. Unless required by state or federal law or in cases of health or safety emergencies, school districts and schools shall not report to the Department the following student data:

(1) Juvenile delinquency records;

(2) Criminal records; or

(3) Medical and health records.

(f) *Restrictions on collecting certain data on students or their families.* Unless required by state or federal law or in cases of health or safety emergencies, school districts and schools shall not collect the following data on students or their families:

(1) Political affiliation;

(2) Voting history;

(3) Income, except as required by law or where a school district or school determines income information is required to apply for, administer, research, or evaluate programs to assist students from low-income families; or

(4) Religious affiliation or beliefs.

(g) *Operators; duties*. An operator shall:

(1) Implement and maintain reasonable security procedures and practices appropriate to the nature of the student data to protect that information from unauthorized access, destruction, use, modification, or disclosure; and

(2) Delete a student's data within a reasonable timeframe not to exceed 45 days if the school district or school requests deletion of data under the control of the school district or school.

(h) *Operators; prohibited activities*. An operator shall not knowingly engage in any of the following activities with respect to such operator's Internet service:

(1) Engage in targeted advertising on the operator's Internet service, or on any other Internet service, when the targeting of the advertising is based upon any information, including student data and state-assigned student identifiers or other persistent unique identifiers, that the operator has acquired because of the use of an

Internet service as described in paragraph (13) of subsection (a) of this section;

(2) Use information, including state-assigned student identifiers or other persistent unique identifiers, created or gathered by an Internet service as described in paragraph (13) of subsection (a) of this section, to amass a profile about a student except in furtherance of K-12 school purposes;

(3) Sell a student's student data. This prohibition does not apply to the purchase, merger, or other type of acquisition of an operator by another entity, provided that the operator or successor entity continues to be subject to the provisions of this section with respect to previously-acquired student data that is subject to this section; or

(4) Disclose student data, unless the disclosure is made:

a. In furtherance of the K-12 school purposes of the Internet service; provided that the recipient of the student data disclosed (i) shall not further disclose the student data unless done to allow or improve the operability and functionality within that student's classroom or school, and (ii) is legally required to comply with the requirements of subsection (g) of this section or paragraphs (1) through (3) of this subsection;

b. To ensure legal or regulatory compliance;

c. To respond to or participate in judicial process;

d. To protect the security or integrity of the operator's Internet service;

e. To protect the safety of users or others or security of the Internet service; or

f. To a service provider, provided that the operator contractually (i) prohibits the service provider from using any student data for any purpose other than providing the contracted service to, or on behalf of, the operator, (ii) prohibits the service provider from disclosing to subsequent third parties any student data provided by the operator, and (iii) requires the service provider to comply with the requirements of paragraphs (1) through (3) of this subsection and to implement and maintain reasonable security procedures and practices as provided in paragraph (1) of subsection (g) of this section.

(5) Notwithstanding paragraph (4) of this subsection, an operator may disclose student data under the following circumstances, so long as paragraphs (1) to (3), inclusive, of this subsection are not violated:

a. If another provision of state or federal law requires the operator to disclose the student data, and the operator complies with the requirements of applicable state and federal law in protecting and disclosing

that information;

b. For legitimate research purposes:

i. As required by state or federal law and subject to the restrictions under applicable state or federal law; or

ii. As allowed by state or federal law and under the direction of a school district, school, or the Department, if no student data is used for any purpose in furtherance of advertising or to amass a profile on the student for purposes other than K-12 school purposes; or

c. To a state agency, school district, or school, for K-12 school purposes, as permitted by state or federal law.

(6) Nothing in this subsection prohibits an operator from using student data as follows:

a. For maintaining, delivering, supporting, evaluating, or diagnosing the operator's Internet service; or

b. For adaptive learning or customized student learning purposes.

(7) Nothing in this subsection prohibits an operator from using or sharing aggregate student data or de-identified student data as follows:

a. For the development and improvement of the operator's Internet service or other educational Internet services;

b. Within other Internet services owned by the operator, and intended for school district, school, or student use, to evaluate and improve educational products or services intended for school district, school, or student use; or

c. To demonstrate the effectiveness of the operator's products or services, including their marketing.

(i) *Exclusions*. This section shall not be construed so as to do any of the following:

(1) Apply to general audience Internet services, even if login credentials created for an operator's Internet service may be used to access those general audience Internet services;

(2) Limit the authority of a law enforcement agency to obtain any content or student data from an operator as authorized by law or pursuant to an order of a court of competent jurisdiction;

(3) Limit Internet service providers from providing Internet connectivity to schools or students and

their families;

(4) Prohibit an operator from marketing educational products directly to parents, so long as the marketing does not result from the use of student data obtained by the operator through the provision of services covered under this section;

(5) Impose a duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications to review or enforce compliance with this section on those applications or software;

(6) Impose a duty upon a provider of an interactive computer service, as defined in § 230 of Title 47 of the United States Code, to review or enforce compliance with this section by third-party content providers;

(7) Impede the ability of a student or parent or guardian to download, transfer, export, or otherwise save or maintain their own student data or documents; or

(8) Prevent the Department, school district, or school from recommending, solely for K-12 school purposes, any educational materials, online content, services, or other products to any student or to the student's family if the Department, school district, or school determines that such products will benefit the student and no person receives compensation for developing, enabling, or communicating such recommendations.

~~(b)~~(j) The provisions of ~~subsection (a)~~subsections (e) through (h) of this section notwithstanding, educational institutions and programs operating in this State, including postsecondary institutions and programs regulated by a state agency, shall disclose to the Department such education records, and student personally identifiable information contained therein, necessary for the audit or evaluation of state and federal education programs in accordance with the terms and conditions of a written agreement negotiated between the Department and each educational institution or program from which education records are sought. Such agreements shall:

(1) State the term of the agreement;

(2) Comply with the requirements of ~~the Family Educational Rights and Privacy Act Regulations set forth in 34 CFR Part 99~~FERPA regarding the Department's use, compilation, maintenance, protection, distribution, re-disclosure and return/destruction of education records obtained hereunder;

(3) Specify the data elements to be disclosed by the educational institution or program;

(4) State the purpose for which the information will be used;

(5) Prohibit any disclosure of education records or student personally identifiable information

contained therein by an educational institution or program in violation of applicable state or federal privacy laws;

(6) Prohibit any modification or amendment except by written agreement duly executed by the parties; and

(7) Contain such additional provisions as agreed upon.

All disclosures required by this subsection shall be for the purpose of ensuring the effectiveness of publicly-funded programs by connecting pre-kindergarten through grade 12 and post-secondary data, and sharing information to improve early childhood and workforce programs as set forth in Delaware's State Fiscal Stabilization Plan and Delaware's Race to the Top Plan, or as otherwise approved by the P-20 Council.

~~(c)~~(k) *Inspection and review of education records*.

(1) All ~~public and private~~ school districts and schools in this State shall allow parents and eligible students to inspect and review the education records of their children or themselves who are, or have been, in attendance at the school. The right to inspect and review ~~educational~~ education records shall be in accordance with this subsection and rules and regulations ~~of~~ promulgated by the Department.

(2) Parents or legal guardians, and eligible students, may request from the school district or school student data included in the student's education record, including student data maintained by an operator, except when the school district or school determines that the requested data maintained by the operator cannot reasonably be made available to the parent.

(3) School districts or charter schools shall provide parents or legal guardians, and eligible students, with an electronic copy of their children's or their own education record upon request, unless the school district or school does not maintain a record in electronic format and reproducing the record in an electronic format would be unduly burdensome.

(4) A parent or eligible student shall have the right to request corrections to inaccurate education records maintained by a school district or school. After receiving a request demonstrating any such inaccuracy, the school district or school that maintains the data shall correct the inaccuracy and confirm such correction to the parent or legal guardians, or eligible student, within a reasonable amount of time.

(5) The Department shall promulgate rules and regulations that:

a. Support school districts and schools in fulfilling their responsibility to annually notify parents or

legal guardians and eligible students of their right to request student data;

b. Assist school districts and schools with ensuring security when providing student data to parents or legal guardians and eligible students;

c. Provide guidance and best practices to school districts and schools in order to ensure that school districts and schools provide student data only to authorized individuals;

d. Support school districts and schools in their responsibility to produce education records and student data included in such education records to parents or legal guardians and eligible students, ideally within three business days of the request;

e. Assist school districts and schools with implementing technologies and programs that allow parents or legal guardians and eligible students to view online, download, and transmit data specific to their children's or their own education record.

f. Enable parents or legal guardians, or eligible students to file a complaint with a school district or school regarding a possible violation of rights under this section or under other state or federal student data privacy and security laws which shall ensure that:

i. Each school district or school designates at least one individual with responsibility to address complaints filed by parents or legal guardians, or eligible students;

ii. The individual designated by the school district or school shall provide a written decision in response to the parent's or legal guardian's or eligible student's complaint; and

iii. A party dissatisfied with the decision may appeal it, first to the superintendent or person of similar position in the school district or school, then, if further appeal is sought, to the board of education or other governing body of the school district or school, and, finally, if further appeal is sought, to the State Board of Education.

~~(d)~~(l) No cause of action or claim for relief, civil or criminal, shall lie or damages be recoverable against any school officer or employee by reason of such officer's or employee's participation in the formulation of ~~such~~ education records or any statements made or of judgments expressed therein concerning a student's academic performance, personal conduct, health, habits, school related activities or potential; nor by reason of the disclosure of ~~the~~ education records or ~~personally identifiable information from~~ student data contained within the education records, nor lack of access thereto, in ~~accordance with subsections (a) through (c) of~~ a manner authorized or

permitted by this section.

Section 2. This Act becomes effective on August 1 following its enactment into law.

Section 3. The provisions of this Act do not apply to projects relating to the privacy and security of student data approved prior to the effective date of this Act under the Department of Education's existing data governance regulation, Regulation 294 of Title 14 of the Delaware Administrative Code.

Section 4. This Act shall be known and may be cited as the "Student Data Privacy Protection Act."

SYNOPSIS

This bill amends Section 4111 of Title 14 of the Delaware Code to establish policies and procedures that enable school districts, schools, teachers, and school staff to collect and use student data for appropriate educational purposes while ensuring that the student data is kept safe and the privacy of students and their parents and guardians is protected.

The bill provides that the Department of Education shall be responsible developing policies and procedures relating to the privacy and protection of student data in accordance with the act, and shall be responsible for ensuring compliance with the act's provisions and with other state and federal data privacy and security laws by the Department, school districts, and schools, including by undertaking certain specified activities.

The bill also establishes the duties and responsibilities of operators of Internet services used for school purposes with respect to student data they collect, including student personally identifiable information.

Further, the bill recognizes the right of parents and eligible students to review and obtain copies of their children's or their own education records and to request the correction of information in the education records which is incorrect or false.

Finally, the bill provides that its provisions will become effective on August 1 the year following its enactment into law, and that its provisions do not apply to projects relating to the privacy and security of student data approved under the Department of Education's existing education record privacy regulation prior to the effective date of the Act.

Author: Senator Sokola