The House Committee on Education offers the following substitute to HB 414:

A BILL TO BE ENTITLED
AN ACT

To amend Chapter 2 of Title 20 of the Official Code of Georgia Annotated, relating to elementary and secondary education, so as to establish and implement policies and requirements with respect to the collection and disclosure of student data; to provide for a short title; to provide for legislative intent and findings; to provide for definitions; to provide for a Department of Education leader to serve as the chief privacy officer; to provide disclosures and requirements for the state data system; to provide for student data collection and reporting restrictions; to provide for a detailed data security plan for the state data system; to provide for restrictions on the use of student data by operators; to provide for parental rights to inspect and correct student data; to provide for rules and regulations; to provide for related matters; to provide for an effective date; to provide for applicability; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Chapter 2 of Title 20 of the Official Code of Georgia Annotated, relating to elementary and secondary education, is amended by revising Article 15, which is reserved, to read as follows:

"ARTICLE 15

20-2-660.

This article shall be known and may be cited as the 'Student Data Privacy, Accessibility, and Transparency Act.'

20-2-661.

(a) The General Assembly acknowledges that student data is a vital resource for parents, teachers, and school staff, and it is the intent of the General Assembly to ensure that

student data is safeguarded and that students' and parents' privacy is honored, respected, and protected.

(b) The General Assembly finds that:

(1) Student data allows parents and students to make more informed choices about educational programs and to better gauge a student's educational progress and needs;

(2) Teachers and school staff utilize student data in planning responsive education programs and services, scheduling students into appropriate classes, and completing reports for educational agencies;

(3) Student information is critical in helping educators assist students in successfully graduating from high school and preparing to enter the workforce or postsecondary education;

(4) In emergencies, certain information should be readily available to school officials and emergency personnel to assist students and their families;

(5) A limited amount of this information makes up a student's permanent record or transcript; and

(6) Student information is important for educational purposes, and it is also critically important to ensure that student information is protected, safeguarded, kept private, and used only by appropriate educational authorities to serve the best interests of the student.

20-2-662.

As used in this article, the term:

(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 is not student personally identifiable information because the local board of education or department or other party has made a reasonable determination that a student's identity is not personally identifiable, whether through single or multiple releases, and taking into account other reasonably available information.

(3) 'Department' means the Department of Education.

(4) 'Education record' means an education record as defined in the Family Educational Rights and Privacy Act (FERPA) and its implementing regulations, 20 U.S.C. Section 1232g; and 34 C.F.R. Part 99.3. An education record does not include the types of student data excepted in FERPA, does not include student data collected by an operator when it is used for internal operations purposes, does not include student data that is not formatted for or expected to be accessed by school, local board of education, or department employees, nor does it include student data that a local board of education determines cannot reasonably be made available to the parent or eligible student.

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

(6) 'K-12 school purposes' means purposes that take place at the direction of the K-12 school, teacher, or local board of education 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.

(7) 'Online service' includes cloud computing services.

(8) 'Operator' means any entity other than the department, local boards of education, the Georgia Student Finance Commission, or schools to the extent that the entity:

(A) Operates an Internet website, online service, online application, or mobile application with actual knowledge that the website, service, or application is used for K-12 school purposes and was designed and marketed for K-12 school purposes to the extent that it is operating in that capacity; and

(B) Collects, maintains, or uses student personally identifiable information in a digital or electronic format.

(9) 'Provisional student data' means new student data proposed for inclusion in the state data system.

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

(11) 'State data system' means the department state-wide longitudinal data system established pursuant to Code Section 20-2-320.

(12) 'Student data' means information regarding a K-12 student who is a resident of this state that is collected and maintained at the individual student level in this state, including but not limited to:

(A) Data descriptive of a student in any media or format, including but not limited to:

(i) The student's first and last name;

(ii) The name of the student's parent or other family members;

(iii) The physical address, email address, phone number, or other information that allows physical or online contact with the student or student's family;

(iv) A student's personal identifier, such as the student number, when used for identification purposes;

(v) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

(vi) State, local, school, or teacher administered assessment results, including participation information;

(vii) 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;

(viii) Attendance and mobility information between and within local school systems in this state;

(ix) The student's sex, race, and ethnicity;

(x) Program participation information required by state or federal law;

(xi) Disability status;

(xii) Socioeconomic information;

(xiii) Food purchases; or

(xiv) Emails, text messages, documents, search activity, photos, voice recordings, and geolocation information; 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, local board of education, or the department or to an operator in the course of the student's or parent's or legal guardian's use of the operator's site, service, or application for K-12 school purposes;

(ii) Is created or provided by an employee or agent of the school or local board of education, including to an operator in the course of the employee's or agent's use of the operator's site, service, or application for K-12 school purposes; or

(iii) Is gathered by an operator through the operation of an operator's site, service, or application for K-12 school purposes.

(13) 'Student personally identifiable data' or 'student personally identifiable information' or 'personally identifiable information' means student data that personally identifies a student that, alone or in combination, is linked to information that would allow a reasonable person who does not have personal knowledge of the relevant circumstances to identify the student.

(14) 'Targeted advertising' means presenting advertisements to a student 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 or single search query without collection and retention of a student's online activities over time.

20-2-663.

(a) The State School Superintendent shall designate a senior department employee to serve as the chief privacy officer of the department to assume primary responsibility for data privacy and security policy, including:

(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) Ensuring that student data contained in the state data system is handled in full compliance with this article, the federal Family Educational Rights and Privacy Act, and other state and federal data privacy and security laws;

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

(4) 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;

(5) Coordinating with the Attorney General's office 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;

(6) 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;

(7) Working with the department general counsel and other officials in engaging with stakeholders about the quality, usefulness, openness, and privacy of data;

(8) 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;

(9) Establishing a model process and policy for any parent to file complaints of privacy violations or inability to access his or her child's education records against the responsible local board of education pursuant to Code Section 20-2-667; and

(10) 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.

(b) The chief privacy officer may investigate issues of compliance with this article and with other state data privacy and security laws by the department and local boards of education and may:

(1) Have access to 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 chief privacy officer under this Code section;

(2) Make such investigations and reports relating to the administration of the programs and operations of the department as are necessary or desirable; and

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

20-2-664.

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 data fields in the state data system to include, but not be limited to:

(A) Any student personally identifiable data required to be reported by state and federal education mandates;

(B) Any student personally identifiable data 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) Develop, publish, and make publicly available policies and procedures for the state data system to comply with this article and other applicable state and federal data privacy and security laws, including the federal Family Educational Rights and Privacy Act. Such policies and procedures 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 local board of education;

(ii) The authorized administrators, teachers, and other school personnel of local boards of education, and the contractors or other authorized entities 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) The authorized staff of the department, and the contractors or other authorized entities 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) The authorized staff of other state agencies in this state as required or authorized by law, including contractors or other authorized entities 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 aggregate data or de-identified data in public reports; and

(C) Consistent with applicable law, criteria for the approval of research and data requests from state and local agencies, the General Assembly, those 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 State Board of Education, not transfer student personally identifiable data to any federal, state, 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 data 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 data 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 data 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 data; 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 the federal Family Educational Rights and Privacy Act, other relevant privacy laws and policies, and the privacy and security policies and procedures developed under the authority of this article, 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 data 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 subparagraph (C) of paragraph (3) of this Code section in the past year regarding the release of student personally identifiable data; 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) Develop policies and procedures to ensure the provision of at least annual notifications to eligible students and parents or guardians regarding student privacy rights under federal and state law.

20-2-665.

(a) Unless required by state or federal law or in cases of health or safety emergencies, local boards of education shall not report to the department the following student data or student information:

(1) Juvenile delinquency records;

(2) Criminal records; or

(3) Medical and health records.

(b) Unless required by state or federal law or in cases of health or safety emergencies, 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 local board of education 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.

20-2-666.

(a) An operator shall not knowingly engage in any of the following activities with respect to such operator's site, service, or application without explicit written consent from the student's parent or guardian, or an eligible student:

(1) Use student data to engage in behaviorally targeted advertising on the operator's site, service, or application or target advertising on any other site, service, or application when the targeting of the advertising is based upon any student data and state-assigned student identifiers or other persistent unique identifiers that the operator has acquired because of the use of such operator's site, service, or application;

(2) Use information, including state-assigned student identifiers or other persistent unique identifiers, created or gathered by the operator's site, service, or application, to amass a profile about a student except in furtherance of K-12 school purposes. For purposes of this paragraph, 'amass a profile' does not include collection and retention of account records or information that remains under the control of the student, parent, or local board of education;

(3) Sell a student's 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 Code section with respect to previously acquired student data that is subject to this article; or

(4) Disclose student personally identifiable data without explicit written or electronic consent from a student over the age of 13 or a student's parent or guardian, given in response to clear and conspicuous notice of the activity, unless the disclosure is made:

(A) In furtherance of the K-12 school purposes of the site, service, or application; provided, however, 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 this article and not use the student information in violation of this article;

(B) To ensure legal or regulatory compliance or protect against liability;

(C) To respond to or participate in judicial process;

(D) To protect the security or integrity of the entity's website, service, or application;

(E) To protect the safety of users or others or security of the site;

(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) requires such service provider to impose the same restrictions as in this paragraph on its own service providers, and (iii) requires the service provider to implement and maintain reasonable security procedures and practices as provided in subsection (b) of this Code section; or

(G) For an educational, public health, or employment purpose requested by the student's parent or guardian, provided that the information is not used or further disclosed for any purpose.

(b) 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 or local board of education requests deletion of data under the control of the school or local board of education.

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

(1) If another provision of federal or state law requires the operator to disclose the student data, and the operator complies with applicable requirements of federal and state law in protecting and disclosing that information;

(2) For legitimate research purposes:

(A) As required by state or federal law and subject to the restrictions under applicable state and federal law; or

(B) As allowed by state or federal law and under the direction of a school, a local board of education, or the department, subject to compliance with subsection (a) of this Code section; or

(3) To a state agency, local board of education, or school, for K-12 school purposes, as permitted by state or federal law.

(d) Nothing in this Code section prohibits an operator from using student data, including student personally identifiable data, as follows:

(1) For maintaining, delivering, developing, supporting, evaluating, improving, or diagnosing the operator's site, service, or application;

(2) Within other sites, services, or applications owned by the operator, and intended for the school or student use, to evaluate and improve educational products or services intended for the school or student use;

(3) For adaptive learning or customized student learning purposes;

(4) For recommendation engines to recommend additional content or services to students within a school service's site, service, or application without the response being determined in whole or in part by payment or other consideration from a third party;

(5) To respond to a student's request for information or for feedback without the information or response being determined in whole or in part by payment or other consideration from a third party; or

(6) To ensure legal or regulatory compliance or to retain such data for these purposes.

(e) Nothing in this Code section prohibits an operator from using or sharing aggregate data or de-identified data as follows:

(1) For the development and improvement of the operator's site, service, or application or other educational sites, services, or applications; or

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

(f) This Code section shall not be construed to 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.

(g) This Code section does not apply to general audience Internet websites, general audience online services, general audience online applications, or general audience mobile applications, even if login credentials created for an operator's site, service, or application may be used to access those general audience sites, services, or applications.

(h) This Code section shall not be construed to limit Internet service providers from providing Internet connectivity to schools or students and their families.

(i) This Code section shall not be construed to prohibit an operator from marketing educational products directly to parents so long as the marketing did not result from the use of student data obtained without parental consent by the operator through the provision of services covered under this Code section.

(j) This Code section shall not be construed to 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 of this Code section on those applications or software.

(k) This Code section shall not be construed to impose a duty upon a provider of an interactive computer service, as defined in Section 230 of Title 47 of the United States Code, to review or enforce compliance with this Code section by third-party content providers.

(l) This Code section shall not be construed to impede the ability of a student or parent or guardian to download, transfer, or otherwise save or maintain their own student data or documents.

(m) Nothing in this Code section or this article prevents the department or local board of education and their employees from recommending, directly or via a product or service, any educational materials, online content, services, or other products to any student or his or her family if the department or local board of education determines that such products will benefit the student and does not receive compensation for developing, enabling, or communicating such recommendations.

20-2-667.

(a) A parent shall have the right to inspect and review his or her child's education record maintained by the school or local board of education.

(b) A parent may request from the school or local board of education student data included in his or her child's education record, including student data maintained by an operator, except when the local board of education determines that the requested data maintained by the operator cannot reasonably be made available to the parent.

(c) Local boards of education shall provide a parent or guardian with an electronic copy of his or her child's education record upon request, unless the local board of education does not maintain a record in electronic format and reproducing the record in an electronic format would be unduly burdensome.

(d) A parent or eligible student shall have the right to request corrections to inaccurate education records maintained by a school or local board of education. After receiving a request demonstrating any such inaccuracy, the school or local board of education that

maintains the data shall correct the inaccuracy and confirm such correction to the parent or eligible student within a reasonable amount of time.

(e) The rights contained in subsections (a) through (d) of this Code section shall extend also to eligible students seeking to access their own education records.

(f) The department shall develop model policies for local boards of education that:

(1) Support local boards of education in fulfilling their responsibility to annually notify parents of their right to request student information;

(2) Assist local boards of education with ensuring security when providing student data to parents;

(3) Provide guidance and best practices to local boards of education in order to ensure that local boards of education provide student data only to authorized individuals;

(4) Support local boards of education in their responsibility to produce education records and student data included in such education records to parents and eligible students, ideally within three business days of the request; and

(5) Assist schools and local boards of education with implementing technologies and programs that allow a parent to view online, download, and transmit data specific to his or her child's education record.

(g)(1) The department shall develop model policies and procedures for a parent or eligible student to file a complaint with a local school system regarding a possible violation of rights under this article or under other federal or state student data privacy and security laws which shall ensure that:

(A) Each local school system designates at least one individual with responsibility to address complaints filed by parents or eligible students;

(B) A written response is provided to the parent's or student's complaint;

(C) An appeal may be filed with the local school superintendent; and

(D) An appeal for a final decision may be made to the local board of education.

(2) Within six months of adoption by the department of model policies and procedures pursuant to paragraph (1) of this subsection, each local board of education shall adopt policies and procedures that include, at a minimum, such department model policies and procedures.

(h) Nothing in this Code section shall authorize any additional cause of action beyond the process described in this Code section or as otherwise authorized by state law.

20-2-668.

(a) The State Board of Education may adopt rules and regulations necessary to implement the provisions of this article.

(b) As of July 1, 2016, any existing collection of student data by the department shall not be considered provisional student data. ~~Reserved.~~"

SECTION 2.

This Act shall become effective on July 1, 2016; provided, however, that to the extent any provision of this Act conflicts with a term of a contract entered into by a state agency, local board of education, or operator in effect prior to July 1, 2016, such provision shall not apply to the state agency, local board of education, or the operator subject to such agreement until the expiration, amendment, or renewal of such agreement.

SECTION 3.

All laws and parts of laws in conflict with this Act are repealed.