HB564

167187-1

By Representatives Mooney, Moore (B), Hanes, Ledbetter, Whorton (I), Butler, Wood, Fridy, Wingo, Fincher, Lee, McMillan, Ingram, Polizos and Holmes (M)

RFD: Education Policy

First Read: 28-APR-15
SYNOPSIS: This bill would set limits on student data that may not be collected and provide what data may be used on a local level to a minimum degree for clearly stated academic purposes.

This bill would set limits on the state government and data collection systems and programs in order to protect students and parents from invasive government practices.

This bill would protect the civil liberties of students and parents which are foundational to strong academics, freedom of speech, and progress.

This bill would limit the collection of certain sensitive information and the disclosure of personally identifiable information to third parties and provide for enforcement and penalties.

A BILL
TO BE ENTITLED
AN ACT
Relating to student data collected in the course of education in Alabama's public education systems; to establish what data may be collected and maintained and to prohibit the State Board of Education, the Department of Education, and other state bodies from compiling or sharing data about students, except under limited circumstances.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. (a) As used in this section, the following terms shall have the following meanings:

(1) AFFECTIVE COMPUTING. Systems and devices that can or attempt to recognize, interpret, process, or simulate aspects of human feelings or emotions.

(2) BIOMETRIC RECORD. A record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual, including fingerprints, retina and iris patterns, voiceprints, DNA sequence, including newborn screening information, facial characteristics, and handwriting.

(3) CLOUD COMPUTING SERVICE. A service that enables on-demand network access to a shared pool of configurable computing resources, e.g., networks, servers, storage, applications, and services, to provide a student, teacher, or staff member account-based productivity applications such as email, document storage, and document editing that can be rapidly provisioned and released with minimal management effort, or cloud computing service provider interaction. A cloud computing service has the characteristics of on-demand
self-service, broad network access, resource pooling, rapid
elasticity, and measured service.

(4) CLOUD COMPUTING SERVICE PROVIDER. An entity,
other than an educational institution, that operates a cloud
computing service.

(5) DEPARTMENT. The Alabama Department of Education.

(6) EDUCATION PROGRAM. A program of instruction
administered by an education agency or education institution
within the state.

(7) ELIGIBLE STUDENT. A student who has reached the
age of majority under Alabama law or attends a school beyond
the high school level to whom rights have transferred.

(8) INTERPERSONAL RESOURCES or INTERPERSONAL SKILLS.
Noncognitive emotional and psychological characteristics and
attributes and skills used to manage relationships and
interactions between or among individuals.

(9) INTRAPERSONAL RESOURCES or INTRAPERSONAL SKILLS.
Noncognitive emotional and psychological characteristics and
attributes used to manage emotions and attitudes within an
individual.

(10) LOCAL EDUCATION AGENCY or LEA. A public board
of education or other public authority legally constituted
within a state for either administrative control or direction
of, or to perform a service function for, public elementary or
secondary schools in a city, county, township, school
district, or other political subdivision of a state, or for a
combination of school districts or counties as are recognized
in a state as an administrative agency for its public elementary schools or secondary schools.

(11) LOCAL EDUCATION INSTITUTION or INSTITUTION. Any public or secondary school.

(12) PARENT. Either the actual biological or adoptive parent of the child or legal guardian of the child.

(13) PERSONALLY IDENTIFIABLE INFORMATION. Information which can be used on its own or with other information to identify, contact, or locate a single person or to identify an individual in context.

(14) PREDICTIVE MODELING. Use of educational data-mining methods to make predictions about future behaviors or performance.

(15) PROCESS or PROCESSING. To use, access, manipulate, scan, modify, transform, disclose, store, transmit, transfer, retain, aggregate, or dispose of student or teacher data.

(16) PSYCHOLOGICAL RESOURCES. Noncognitive, emotional characteristics, attributes, and skills, including mindsets, learning strategies, and effortful control, used by an individual to address or manage various life situations.

(17) STATE AGENCIES. The Alabama Department of Education, the State Board of Education, or any regional education service agency, or any other state education entity which operates or serves the entire state.

(18) STUDENT DATABASE. The Alabama Statewide Longitudinal Data System, as well as any other data warehouse
containing Alabama student information, including regional, interstate, or federal data warehouse organizations under contract to or with a memorandum of understanding with the Department of Education.

(19) TEACHER RECORDS. Applies to teachers, paraprofessionals, principals, and other administrators and shall mean the following:

a. Social Security number.
b. Name.
c. Address.
d. Birthdate.
e. Email address and telephone number.
f. Compensation information.
g. Resume information.
h. Performance evaluations.
i. Other information that, alone or in combination, is linked or linkable to a specific staff member that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the staff member with reasonable certainty.

(20) TERRY SEARCH. A onetime search for weapons or items prohibited by the school which includes a pat down of outer clothing only and the search must take place at entrance to the school only.

(21) TRACK. To collect and maintain records of a student's activities once he or she exits the educational
system, including, but not limited to, his or her entrance into and progression through the workforce or the military.

(22) WORKFORCE INFORMATION. Information related to unemployment insurance (UI), wage records, UI benefit claims, or employment and earnings data from workforce data sources, such as state wage records, or the Federal Employment Data Exchange System (FEDES).

(23) WRITTEN CONSENT. Written consent given within six months before the data collection or disclosure consented to, specifically referencing that data collection or disclosure, and dated and signed on the same day.

(b) Types of data that may be utilized on a local level include:

(1) The student data that may only be collected on a local level by an educational institution without the written consent of parents of students who are enrolled in a public school in Alabama shall be limited to the following:
   a. Name and address.
   b. State and national assessment results.
   c. Course taking and completion and credits earned.
   d. Course grades and grade point average.
   e. Date of birth, grade level, and expected graduation date/graduation cohort.
   f. Degree, diploma, or credential attainment.
   g. Enrollment.
   h. Attendance and transfers.
i. Medical records limited to immunization records required by state law, records needed or created by a school-based health professional for administering prescription drugs or otherwise treating a student at school, records needed or created by a school-based counselor when a student seeks counseling while at school, or records required by the Individuals with Disabilities Education Act, 20 U.S.C. Section 1400, et seq.

j. Discipline reports limited to objective information sufficient to produce the Title IV Annual Incident Report pursuant to the Clery Act, 20 U.S.C. Section 1092(f).

k. Juvenile delinquency or other criminal or correctional records if necessary to meet the educational needs of the student or to ensure the safety of staff or students, provided that an institution of higher education may collect records sufficient to produce the Title IV Annual Incident Report pursuant to the Clery Act, 20 U.S.C. Section 1092(f).

l. Remediation data.

m. Special education data, limited to data required by the Individuals with Disabilities Education Act, 20 U.S.C Section 1400 et seq.

n. Data limited to that required by the Elementary and Secondary Education Act.

o. Student workforce information is limited to information related to work-study programs participated in for academic credit.
p. Student or family Social Security numbers only if needed by an institution of higher education to comply with state or federal law.

q. Student or family income data, limited to data required by law to determine eligibility to participate in or receive financial assistance under a program.

r. Information about extracurricular activities, limited to activities that are school-sponsored or engaged in for academic credit.

(2) Unless explicitly mandated by federal statute, a local education agency or education institution must obtain written informed consent from parents or eligible students before collecting any data points other than those listed in subsection (1), including, but not limited to, the following:

a. Medical, health, including height, weight, and body mass index, and mental health records, except as provided in paragraph (b)(1)i.

b. Student or family workforce information, except as provided in paragraph (b)(1)o.

(3) No funds from any source shall be used on construction, enhancement, or expansion of any data system that does not comply with these limitations, or that is designed to track students beyond their K-12 or postsecondary education careers or compile their personal, nonacademic information beyond what is necessary for either administrative functions directly related to the student's education, or evaluation of academic programs and student progress.
(4) No state agency or education institution shall pursue or accept any grant, whether from the federal government or any private entity, that would require collecting or reporting any types of data in violation of this subsection.

(5) Only aggregate data will be transmitted from a local education agency to state.

(6) Any PII currently residing within the SDLS shall be destroyed.

(c) TRANSPARENCY OF DATA SYSTEM.

(1) State agencies and educational institutions shall publicly and conspicuously disclose on their websites the existence and character of any form of education records or teacher records maintained by the agencies or educational institutions, directly or through contracts with outside parties. Local educational institutions shall annually notify parents, eligible students, and teachers of this website posting. Local agencies shall also provide annual electronic notification of this information to the Chairs of the Senate Education Committee and House Education Committee. Such disclosure and electronic notifications shall include the following:

a. The legal authority that authorizes the establishment and existence of the data repository.

b. The principal purpose or purposes for which the information is intended to be used.
c. The categories of individuals on whom records are maintained in the data repository.

d. The categories of records maintained in the data repository.

e. Each expected disclosure of the records contained in the data repository, including the categories of recipients and the purpose of such disclosure.

f. The policies and practices of the state agency or educational institution regarding storage, irretrievability, access controls, retention, and disposal of the records.

g. The title and business address of the official who is responsible for the data repository, and the name and business address of any contractor or other outside party maintaining the data repository for or on behalf of the state agency or education institution.

(2) State education agencies shall use only aggregate data in published reports.

Section 2. No state or national student assessment shall be adopted or administered in this state that collects any type of psychological data, including assessment of noncognitive skills or attributes, psychological resources, mindsets, learning strategies, effortful control, attitudes, dispositions, social skills, or other interpersonal or intrapersonal resources.

Section 3. No state agency, district board of education, or pre K-12 educational institution shall administer any student survey, assessment, analysis,
evaluation, or similar instrument that solicits information about the student or the student's family concerning the following:

(1) Political affiliations or beliefs.
(2) Mental or psychological problems, psychological resources, mindsets, learning strategies, effortful control, attributes, dispositions, social skills, attitudes, or intrapersonal resources.
(3) Sexual behavior or attitudes.
(4) Illegal, antisocial, self-incriminating, or demeaning behavior.
(5) Critical appraisals of another individual with whom a student has a close family relationship.
(6) Legally recognized privileged or analogous relationships, such as those with a lawyer, physician, therapist, psychotherapist, or clergyman.
(7) Religious practices, affiliations, or beliefs.
(8) Personal or family gun ownership.
(9) Income or other income-related information except that required by law to determine eligibility to participate in or receive financial assistance under a program.
(10) Language spoken in student's home.
(11) Criminal records of family members.
(12) Student biometric records.
(13) Any data collected via affective computing, including analysis of facial expressions, EEG brain wave
patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking.

(14) Any data, including any resulting from state or national assessments, that measure psychological resources, mindsets, learning strategies, effortful control, attributes, dispositions, social skills, attitudes, or intrapersonal resources.

(15) Any data collected through predictive modeling.

Section 4. (a) Subject to the exceptions contained in this act, access to student education records in the student database shall be restricted to the authorized representatives of the local agency or education institution who require such access to perform their assigned duties. No party may be designated an authorized representative unless that party is on the staff and under the direct control of the designating state agency or institution.

(b) Subject to the exceptions contained in this act, no personally identifiable student or teacher data shall be disclosed without the written consent of the parents or eligible students.

(c) RESEARCH AND STUDIES.

(1) The department may develop and publish criteria for the approval of research-related data requests from state and local governmental agencies, the Legislature, academic researchers, and the public. Only aggregate data may be provided for such requests.
(2) The data request and process shall be administered in a full and equal manner to all academic researchers and the public.

(3) Personally identifiable information from an education record of a student, or from teacher records, may not be released to a party conducting studies for or on behalf of the local educational agencies or educational institutions without the written consent of the parent or eligible student except to:

a. Administer assessments.

b. Administer student aid programs provided that the outside party conducting the study meets all the requirements for contractors set forth in subsection (e).

(d) AUDITS, EVALUATIONS, AND COMPLIANCE.

In conducting any audit or evaluation of an education program, the State Board of Examiners of Public Accounts or any compliance or enforcement activity in connection with legal requirements that relate to state or district supported education programs, when such audit, evaluation, or activity involves access to personally identifiable student or teacher information, education records and teacher records may be released only to authorized representatives of state education agencies, local boards of education, or institutions. No party may be designated an authorized representative unless that party is on the staff and under the direct control of the designating state education agency, district board, or institution.
(e) OUTSOURCING.

(1) Local education agency, district boards of education, and institutions may not disclose personally identifiable information from education records or teacher records without the written consent of parents or eligible students, to a contractor, consultant, or other party to whom the local agency, district board, or institution has outsourced institutional services or functions unless that outside party:

a. Performs an institutional service or function for which the local education agency or institution would otherwise use its employees.

b. Is under the direct control of the local agency or institution with respect to the use and maintenance of education records or teacher records.

c. Limits internal access to education records or teacher records to those individuals who require access to those records for completion of the contract that in no way conflicts with this act.

d. Does not use the education records or teacher records for any purposes other than those explicitly authorized in the contract which in no way conflicts with this act.

e. Does not disclose any personally identifiable information from education records or teacher records to any other party:
1. Without the written consent of the parent or eligible student.

2. Unless required by statute or court order and the party provides a notice of the disclosure to the local education agency, or institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by the statute or court order.

f. Maintains administrative, technical, and physical safeguards to actually protect the security, confidentiality, and integrity of the personally identifiable student or teacher data in its custody.

g. Uses encryption technologies to protect data while in motion or in its custody from unauthorized disclosure using a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5.

h. Has sufficient administrative and technical procedures to monitor continuously the security of personally identifiable student or teacher data in its custody.

i. Conducts a security audit annually and provides the results of that audit to each state agency, district board, or institution that provides education records or teacher records.

j. Provides the state agency, district board, or institution with a breach-remediation plan which does not conflict with this act and is acceptable to the state agency,
district board, or institution before initial receipt of
education records or teacher records.

k. Reports all suspected security breaches to the
local education agency or institution that provided education
records or teacher records as soon as possible but not later
than 48 hours after a suspected breach was known or would have
been known by exercising reasonable diligence.

l. Reports all actual security breaches to the
Attorney General, state agency, district board, or institution
that provided education records as soon as possible but not
later than 24 hours after an actual breach was known or would
have been known by exercising reasonable diligence.

m. In the event of a security breach or unauthorized
disclosure of personally identifiable information, pays all
costs and liabilities incurred by the state agency, district
board, or institution related to the security breach or
unauthorized disclosure, including, but not limited to, the
costs of responding to inquiries about the security breach or
unauthorized disclosure, of notifying subjects of personally
identifiable information about the breach, of mitigating the
effects of the breach for the subjects of the personally
identifiable information, and of investigating the cause or
consequences of the security breach or unauthorized
disclosure.

n. Returns to the local education association or
institution all personally identifiable information in its
custody at the termination of the contract.
(f) ACTIONS REQUIRED IN CASE OF SECURITY BREACH OR UNAUTHORIZED DISCLOSURE.

In the event of a security breach or unauthorized disclosure of personally identifiable student or teacher data, whether by a state agency, district board, or educational institution, or by a third party given access to education records or teacher records pursuant to subsections (c), (d), or (e), the state agency, district board, or education institution shall do all of the following:

(1) Immediately notify the subjects of the breach or disclosure.

(2) Report the breach or disclosure to the Family Policy Compliance Office of the U. S. Department of Education.

(3) Allow the Attorney General and district attorneys access to investigate the causes and consequences of the breach or disclosure.

(g) COMMERCIAL USE PROHIBITED.

(1) Personally identifiable information from education records or teacher records may not be disclosed to any party for a commercial use, including, but not limited to, marketing products or services, compilation of lists for sale or rental, development of products or services, or creation of individual, household, or group profiles.

(2) Any cloud computing service provider performing services for a state agency, district board, or institution is prohibited from using information from education records or teacher records for any secondary purposes that benefit the
cloud computing service provider or any third party, including, but not limited to, online behavioral advertising, creating or correcting an individual or household profile primarily for the cloud computing service provider's benefit, the sale of the data for any commercial purpose, or any other similar commercial for-profit activity; provided, however, that a cloud computing service provider may process or monitor student data solely to provide such service to the state agency, district board, or institution, and to maintain the integrity of such service.

(3) Any cloud computing service provider that enters into an agreement to provide cloud computing services to a state agency, district board, or institution shall certify in writing to that state agency, district board, or institution that it will comply with the terms and conditions set forth in subsection (e); and that the state agency, district board, or institution maintains ownership of all student and teacher data.

(4) Any student or teacher data stored by a cloud computing service provider shall be stored within the boundaries of the United States.

(h) PREDICTIVE MODELING PROHIBITED.

No student data shall be used for predictive modeling for detecting behaviors, beliefs, or value systems, or predicting or forecasting student outcomes.

(i) LIMITATIONS ON VIDEO OR AUDIO MONITORING.
There shall be no video or audio monitoring of classrooms for any purpose, including for teacher evaluation, without the approval of the district school board after public hearings and the written consent of the teacher, of all eligible students, and of the parents of all other students in the classroom.

(j) INTERAGENCY DISCLOSURE PROHIBITED.

Personally identifiable information from education records or teacher records may not be disclosed to any non-education governmental agency, including, but not limited to, the Alabama Department of Labor, whether within or outside the state, or to any party that intends to use or disclose the information or data for the purpose of workforce-development or economic planning.

(k) LIMITATIONS ON INTERSTATE DISCLOSURE.

Subject to the provisions of subsections (c), (d), (e), (m), and this subsection, personally identifiable information from education records or teacher records may not be disclosed to any governmental agency or other entity outside the state, except disclosure may be made in the following circumstances:

(1) To an institution attended by a student who has transferred out of state.

(2) To an out-of-state program in which a student voluntarily participates and for which such a data transfer is a condition or requirement of participation.
(3) When a student is classified as a migrant for federal reporting purposes.

(1) LIMITATIONS ON DISCLOSURE TO FEDERAL GOVERNMENT.

(1) No personally identifiable information from education records or teacher records may be disclosed to any federal agency, including the U. S. Department of Education or the U. S. Department of Labor or their representatives, only aggregate data may be provided.

(2) No information or data collected may be sold or distributed to third parties or to other government agencies, federal or state, about any student in Alabama's public schools system that has been collected through Alabama's public schools or during a student's participation in an Alabama public school activity. No research data collected regarding individual students by Alabama's public schools may be sold to third parties in return for money or supplies in Alabama's public schools. Any violation of this subdivision will result in a strict liability for the violating party or parties. Any student whose data is sold that has been collected by the school or a state educational agency or employee will have standing to sue for damages regardless of the profit from the data.

(m) DISCLOSURE TO ASSESSMENT CONSORTIUM OR COMPANY.

State agencies, district boards, or institutions shall not disclose student or teacher information to any assessment consortium of which the state is a member, or company with which the state contracts for development and
administration of any assessment, unless all of the following are met:

(1) The information is transmitted in non-individual record format.

(2) The information is limited to information directly related to the assessment, such as a student's grade level and test scores.

(3) No psychological information of any kind, including that listed in Section 2, is included as part of the test scores.

(n) DESTRUCTION OF DATA.

An educational institution shall destroy and remove from the student database all education records of a student within five years of the student's graduation from that institution, provided that the institution may retain records showing dates of attendance, diploma, degree, or degrees received, and contact information. If a student withdraws from an educational institution before graduating, the institution, within one year of the student's withdrawal, shall destroy and remove from the database all education records of that student except records showing dates of attendance.

Section 5. (a) The Legislature presupposes parental authority over the education of their children and personal information regarding their children; therefore, all student academic materials and records shall be made available to parents or eligible students upon request and without question.
(b) Parents or eligible students shall have the right to access their student's information that is held in any education database and a right to request the correction or removal of data within those student records. Upon receiving a written request from a parent to the local board or institution that states the information believed to be in error or inappropriate, the institution shall expeditiously correct or remove all information found to be in error or inappropriate. Any public school official or district that refuses to provide information about the child's education or any other data compiled on the child to parents or ignores a written request for student information is in clear violation of this act and is committing a strict liability offense.

(1) A parent has a right not only to the education record, meaning any material the school holds on the specific student, but also to the curriculum and any programs implemented or curriculum used in the school.

(2) Anything that is accessible online by any Alabama public school personnel about a specific student in file or records of the students must be viewable at all times by the parent or eligible student online. The parent or eligible student must also be able to view the information physically by visiting the school because not all parents have access to the Internet. Parents must be able to view this information during normal business hours at no charge to the parent or eligible student. A parent or eligible student must be able to keep his or her own personal copy of the record and
take the copy of the official record off school grounds. A copy of the student's record must be provided free of charge to the parent or eligible students, if requested.

(c) No student shall be required to complete any questionnaire, survey, or assessment regarding personal habits or attitudes or activities without written informed parental permission obtained in advance of administering any such questionnaire or assessment. Such permission document must include a complete copy of the questionnaire, survey, or assessment.

(d) No student shall be denied services in Alabama's public schools because the student's parent requested information of any kind about his or her child's education.

(e) Re-disclosure of personally identifiable information to any third party is forbidden without informed consent of a parent or legal guardian.

(f) No student shall be arrested, seized, or searched without probable cause or proper warrant issued from a court with proper jurisdiction. No student's personal property may be seized or searched without probable cause or proper warrant. Personal property includes student's email accounts regardless of whether or not it is a school email account or one controlled by a private company. Any digital correspondence created by a student on his or her personal laptop or another device, any documents stored on computer or electronic devices of any type owned by a student, cell phone or home phone records on the student's electronic devices may
not be searched or seized without probable cause or a warrant. Any online account in which the student must use a user name or email and password creates an expectation of privacy regardless of whether public or privately controlled. A proper warrant or probable cause must be established to search or seize information or data from any of these accounts used by the student or which are associated with the student's name. No student locker may be searched without probable cause or proper warrant. No student may be questioned or interrogated by law enforcement without the presence of either his or her attorney or a parent.

(g) The only time a student may be searched in school without warrant or probable cause is to a minimum degree for security purposes only if the school has established metal detectors or a security check point at the entrance to the school. This search must be limited to searching for the school's prohibited items that impact safety. Nothing obtained in these searches that is illegal or in violation of school rules may be used as evidence or appear in official school record against the student or court regardless of who performs these searches. If the student objects to body scans for health or privacy reasons then a terry search must be offered as an alternative to full body scans or metal detectors.

Section 6. (a) No student shall be denied access to any public educational service or grade advancement in Alabama public schools whose parent, guardian, or eligible student who
decides not to participate in or utilize any assessments, career counseling, workshops, psychological counseling session, or other activities that the parent or guardian deems inappropriate or offensive.

(b) A parent or eligible student shall notify the school in writing and name what program or programs he or she chooses not to participate in as outlined in subsection (a) of Section 5.

(c) A parent or eligible student must have a sound academic alternative.

Section 7. (a) Each violation of any provision of this act by an organization, state agency, a district board of education, or an institution as defined in this subsection shall be punishable by a civil penalty of up to one thousand dollars ($1,000); a second violation by the same organization or entity involving the education records and privacy of the same student shall be punishable by a civil penalty of up to five thousand dollars ($5,000); any subsequent violation by the same organization or entity involving the education records and privacy of the same student shall be punishable by a civil penalty of up to ten thousand dollars ($10,000); and each violation involving a different individual education record or a different individual student shall be considered a separate violation for purposes of civil penalties.

(b) The Attorney General or a district attorney shall have the authority to enforce compliance with this act by investigation and subsequent commencement of a civil
action, to seek civil penalties for violations of this section, and to seek appropriate injunctive relief, including, but not limited to, a prohibition on obtaining personally identifiable information for an appropriate time period. In carrying out such investigation and in maintaining such civil action, the Attorney General or any deputy or assistant attorney general or a district attorney is authorized to subpoena witnesses, compel their attendance, examine them under oath, and require that any books, records, documents, papers, or electronic records relevant to the inquiry be turned over for inspection, examination, or audit; subpoenas issued pursuant to this subsection may be enforced pursuant to the civil practice law and rules.

(c) This act creates a private right of action for parents, eligible students, and Alabama citizens to enforce this act and seek civil damages for violations of this act. Parents and students and Alabama citizens may seek appropriate injunctive relief from any governmental agency or governmental branch, including, but not limited to, a prohibition on obtaining personally identifiable information for an appropriate time period. Alabama citizens may also seek injunctive relief against private businesses for violating any part of this act. Parents and eligible students and Alabama citizens will be able to sue in their own accord for violations of the act without regard to actions taken by the Attorney General or district attorney. The same penalties
outlined in subsection (a) of Section 7 will be available to private citizens, eligible students, and parents.

Section 8. The provisions of this act are severable. If any part of this act is declared invalid or unconstitutional, that declaration shall not affect the part which remains.

Section 9. This act shall become effective July 1, 2015, and shall apply beginning with the 2015-2016 academic year.