SB318

173186-1

By Senators Reed, Figures, Ross, Pittman, Allen and Waggoner

RFD: Education and Youth Affairs

First Read: 01-MAR-16
SYNOPSIS: This bill would establish the Alabama Student and Parent Privacy Protection Act.

This bill would limit the collection and disclosure of information relating to public school students and teachers to academic purposes.

This bill would provide civil penalties for violations.

A BILL
TO BE ENTITLED
AN ACT

Relating to public prekindergarten, elementary, and secondary education; to limit the collection and disclosure of student and teacher information to specific academic purposes; and to provide civil penalties for violations.

BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

Section 1. This act shall be known and may be cited as the Alabama Student and Parent Privacy Protection Act.
Section 2. For the purposes of this act, 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, but not limited to, fingerprints; retina and iris patterns; voiceprints; DNA sequence, including newborn screening information; facial characteristics; and handwriting, unless handwriting for cursive academic assignment.
3. CLOUD-BASED COMPUTING SERVICE. A service that enables on demand network access to a shared pool of configurable computing resources such as 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 may 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. DEPARTMENT. The State Department of Education.
5. EDUCATION PROGRAM. A program of instruction administered by a local education agency or local education institution within the state.
(6) ELIGIBLE STUDENT. A student who has reached the age of majority under Alabama law or attends a local education institution beyond the high school level to whom rights have transferred.

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

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

(9) LOCAL EDUCATION AGENCY. A public city or county board of education or other public authority legally constituted within the 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 the state, or for a combination of school districts or counties as are recognized in the state as an administrative agency for its public elementary schools or secondary schools.

(10) LOCAL EDUCATION INSTITUTION. Any public prekindergarten, elementary, or secondary school.

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

(12) PERSONALLY IDENTIFIABLE STUDENT INFORMATION. One or more of the following:
a. The name of a student.
b. The name of the parent or other family member of
   the student.
c. The address of a student or the parent or other
   family member of the student.
d. A photograph, video, or audio recording that
   contains an image of or the voice of the student.
e. Indirect identifiers including, but not limited
to, the date of birth, place of birth, maiden name of the
mother of, Social Security number, student number, biometric
record, telephone number, credit card account number,
insurance account number, financial services account number,
customer number, persistent online identifier, email address,
personal social media account address, and other electronic
address of the student.
f. Any aggregate or deidentified student data that
   is capable of being deaggregated or reconstructed to the point
   that an individual student may be identified.
g. Any student data or other information that, alone
   or in combination, is linked or linkable to a specific student
   that would allow a reasonable person, who does not have
   personal knowledge of the relevant circumstances, to identify
   a specific student with reasonable certainty.

(13) PERSONAL SOCIAL MEDIA ACCOUNT. An account with
an electronic medium or service where users may create, share,
and view user-generated content including, but not limited to,
uploading or downloading videos or still photographs, blogs,
video blogs, podcasts, messages, emails, or Internet website profiles or locations. The term does not include an account opened at the request of a local education institution, or provided by a local education institution, and intended to be used solely on behalf of the local education institution.

(14) PREDICTIVE MODELING. The 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) SPECIFIC CONTENT. Data or information on a personal social media account that is identified with sufficient particularity to demonstrate prior knowledge of the details of the content and distinguish the content from other data or information on the account with which the account may share similar characteristics.

(18) STATE AGENCIES. The department, the State Board of Education, or any regional education service agency, or any other state education entity which operates or serves the entire state.
(19) 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, any local education institution, or local education agency.

(20) STUDENT INFORMATION SYSTEM. A software application or cloud-based computing service, or both, that allows a local education institution to input, maintain, manage, or retrieve student data, or personally identifiable student information, including applications that track or share personally identifiable student information in real time.

(21) STUDENT INFORMATION SYSTEM PROVIDER. An entity that sells, leases, provides, operates, or maintains a student information system for the benefit of a local education institution.

(22) TEACHER RECORDS. Information pertaining to teachers, paraprofessionals, principals, and other administrators that includes, but is not limited to, any of the following:

a. Social Security number.

b. Name.

c. Address.

d. Birthdate.

e. Email address.
f. Telephone number.

g. Compensation information.

h. Resume information.

i. Performance evaluations.

j. Other information that, alone or in combination, is linked or linkable to a specific staff member that would allow a reasonable person in the local education institution community, who does not have personal knowledge of the relevant circumstances, to identify the staff member with reasonable certainty.

(23) TERRY SEARCH. A onetime search for weapons or items prohibited by the local education institution which includes a pat down of outer clothing only and is conducted only at the main entrance to the local education institution.

(24) TRACK. To collect and maintain records of the activities of a student after 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.

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

(26) WRITTEN CONSENT. Consent, in writing, given within six months before the data collection or data disclosure consented to, specifically referencing the precise type of data collection or data disclosure that is being
consented to, and dated and signed on the same day. The term
does not include general, nonspecific consent to collect or
disclose data.

Section 3. (a) Student data that may only be
collected at the local level by a local education institution,
and without the written consent of the parent of a student who
is enrolled in a local education institution in the state,
shall be limited to the following:

(1) Name or address, or both.
(2) State and national assessment results.
(3) Course taking and completion, and credits earned.
(4) Course grades and grade point average.
(5) Date of birth, grade level, and expected graduation date or graduation cohort.
(6) Degree, diploma, or credential attainment.
(7) Enrollment.
(8) Attendance and transfers.
(9) Medical records limited to immunization records required by state law, records needed or created by a local education institution-based health professional for administering prescription drugs or otherwise treating a student at a local education institution, records needed or created by a local education institution-based counselor when a student seeks counseling while at the local education institution, or records required by the Individuals with Disabilities Education Act, 20 U.S.C.A. Section 1400 et seq.
(10) Discipline reports limited to objective information about disciplinary incidents or, for institutions of higher education, objective information sufficient to produce the Title IV Annual Incident Report pursuant to the Clery Act, 20 U.S.C.A. Section 1092(f).

(11) Juvenile delinquency or other criminal or correctional records only if necessary to meet the educational needs of the student or to ensure staff or student safety, 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.A. Section 1092(f).

(12) Remediation data.

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

(14) Data limited to that required by the Elementary and Secondary Education Act.

(15) Student workforce information is limited to information related to work study programs participated in for academic credit.

(16) Student or family Social Security numbers only if needed by an institution of higher education to comply with state or federal law.

(17) Student or family income data, limited to data required by law to determine eligibility to participate in or receive financial assistance under a program.
(18) Information about extracurricular activities, limited to activities that are local education institution-sponsored or engaged in for academic credit.

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

(1) Medical; health, including height, weight, and body mass index; and mental health records, except as provided in subdivision (9) of subsection (a).

(2) Student or family workforce information, except as provided in subdivision (15) of subsection (a).

(c) No funds from any source shall be used on construction, enhancement, maintenance, 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 education of the student, or the evaluation of academic programs and student progress.

(d) No state agency or local education institution shall pursue or accept any grant, whether from the federal government or any private entity, that would require the
collecting or reporting of any type of data in violation of
this section.

(e) Only aggregate data may be transmitted from a
local education agency to state.

(f) Any personally identifiable student information
on current students discovered within the Alabama Statewide
Longitudinal Data System shall be destroyed.

Section 4. (a) State agencies and education
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 education institutions, directly or through
contracts with outside parties. Local education 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 and Youth Affairs Committee and
the House Education Policy Committee. The disclosure and
electronic notifications shall include all of the following:

(1) The legal authority that authorizes the
establishment and existence of the data repository.

(2) The principal purpose or purposes for which the
information is intended to be used.

(3) The categories of individuals on whom records
are maintained in the data repository.

(4) The categories of records maintained in the data
repository.
(5) Each expected disclosure of the records contained in the data repository, including the categories of recipients and the purpose of such disclosure.

(6) The policies and practices of the state agency or local education institution regarding storage, irretrievability, access controls, retention, and disposal of records.

(7) 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 local education institution.

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

Section 5. No state assessment, including 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, effortful control, attitudes, dispositions, social skills, or other interpersonal or intrapersonal resources.

Section 6. No state agency, local education agency, or local education institution shall administer any student survey, assessment, analysis, evaluation, or similar instrument that solicits information about the student or the family of the student concerning any of the following:

(1) Political affiliations or beliefs.
(2) Noncognitive and nonacademic mental or psychological problems, psychological resources, mindsets, effortful control, attributes, dispositions, social skills, attitudes, or intrapersonal resources.

(3) Sexual behavior or attitudes unless the student is receiving medical care or physiological care from a licensed medical professional.

(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 clergy.

(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 the home of a student unless required by federal law, which shall be cited when the data is collected.

(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 data resulting from state or national assessments, that measure psychological resources, mindsets, effortful control, attributes, dispositions, social skills, attitudes, or intrapersonal resources.

(15) Any data collected through predictive modeling.

Section 7. (a) Subject to the exceptions contained in this act, access to student education records in a student information system shall be restricted to the authorized representatives of the local education agency or local education institution who requires access to perform their assigned duties. No individual may be designated as an authorized representative unless he or she is on the staff or under the direct control of the designating state agency, local education agency, or local education institution.

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

(c)(1) The department may develop and publish criteria for the approval of research-related data requests from state and local governmental agencies, the Legislature, and academic researchers, and may allow release in accordance with that criteria. 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 student 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 local education agencies or local education institutions without the written consent of the parent or eligible student, except to do either of the following:

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) In conducting any audit or evaluation of an education program, the Department of Examiners of Public Accounts, or any compliance or enforcement agency in connection with legal requirements that relate to state-supported or local education agency-supported education programs, when the audit, evaluation, or activity involves access to personally identifiable student information or teacher records, education records and teacher records may be released only to authorized representatives of state education agencies, local education agencies, or local education institutions. No individual may be designated as an authorized representative unless he or she is on the staff or under the direct control of the designating state agency, local education agency, or local education institution.
(e)(1) Local education agencies and local education institutions may not disclose personally identifiable student information from education records or teacher records, without the written consent of the parent or eligible student, to a contractor, consultant, or other party to whom the local education agency or local education 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 local education institution would otherwise use its employees.

b. Is under the direct control of the local education agency or local education institution, or on the staff with respect to the use and maintenance of education records or teacher records including, but not limited to, a student information system provider.

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 purpose other than those explicitly authorized in the contract, which in no way conflicts with this act.

e. Does not disclose any personally identifiable student 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 local education institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by statute or court order.

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

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

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

k. Reports all suspected security breaches to the state agency, local education agency, or local education 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 should have been known by exercising reasonable diligence.

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

m. In the event of a security breach or unauthorized disclosure of personally identifiable student information, pays all costs and liabilities incurred by the state agency, local education agency, or local education 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 student information about the breach, of mitigating the effects of the breach for the subjects of the personally identifiable student information, and of investigating the cause or consequences of the security breach or unauthorized disclosure.
n. Returns to the state agency, local education agency, or local education institution all personally identifiable student information in its custody at the termination of the contract.

(f) In the event of a security breach or unauthorized disclosure of personally identifiable student information or teacher records, whether by a state agency, local education agency, or local education institution, or by a third party given access to education records or teacher records pursuant to subsection (c), (d), or (e), the state agency, local education agency, or local 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 United States Department of Education.

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

(g)(1) Personally identifiable student 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 student information system provider performing services for a state agency, local education agency, or local education institution is prohibited from using information from education records or teacher records for any secondary purposes that benefit the student information system provider or any third party including, but not limited to, online behavioral advertising, creating or correcting an individual or household profile primarily for the benefit of the student information system provider, the sale of the data for any commercial purpose, or any other similar commercial for-profit activity. A student information system provider may process or monitor student data solely to provide such service to the state agency, local education agency, or local education institution, and to maintain the integrity of the service.

(3) Any student information system provider that enters into an agreement to provide a student information system to a state agency, local education agency, or local education institution shall certify in writing to that state agency, local education agency, or local education institution that the student information system provider shall comply with the terms and conditions set forth in subsection (e) and that the state agency, local education agency, or local education institution maintains ownership of all student and teacher records.
Any student or teacher records stored by a student information system provider shall be stored within the boundaries of the United States.

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

(i) There shall be no video or audio monitoring of classrooms for any purpose, including for teacher evaluation, without the approval of the local education agency 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) Personally identifiable student information from education records or teacher records may not be disclosed to any noneducation government agency including, but not limited to, the Alabama Department of Labor, whether within or outside the state, or to any person that intends to use or disclose the information or data for the purpose of workforce development or economic planning.

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

(1) To a local education 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 the data transfer is a condition or requirement of participation.

(3) When a student is classified as a migrant for federal reporting purposes.

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

(2) No personally identifiable student information collected may be sold or distributed to third parties or to other government agencies, federal or state, about any student in the public school system of the state that has been collected through the public school system or during the participation of the student in a state public school activity. No research data collected regarding individual students by the state public schools may be sold to third parties in return for money or supplies in those public schools. Any violation of this section shall result in a strict liability for the violating party or parties. Any student whose data is sold that has been collected by the state agency, local education agency, local education institution, or employee of any of these, shall have standing to sue for damages regardless of the profit made off of the data.
(m) State agencies, local education agencies, or local education institutions may not disclose personally identifiable student information or teacher records to any assessment consortium of which the state is a member, or company with which the state contracts for development or administration of any assessment, or both, unless:

(1) The information is transmitted in nonindividual record format.

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

(3) No psychological information of any kind, including that listed in Section 4, is included as part of the test scores.

(n) A local education institution shall destroy and remove from the student database all education records of a student within five years after the graduation of the student from that local education institution, provided that the local education institution may retain records showing dates of attendance, grades, diploma or degrees received, and contact information. If a student withdraws from a local education institution before graduating, the local education institution, within one year after the withdrawal, shall destroy and remove from the student database all education records of that student, except records showing dates of attendance and grades.
Section 8. (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 available to parents or eligible students upon request and without question.

(b) Parents or eligible students may access any information regarding their students, or themselves, that is held in any student information system, or student information system provider's student database, and may request the correction or removal of data within those student records. Upon receiving a written request from a parent or eligible student to remove data believed to be in error or held in violation of this act, the local education agency or local education institution shall expeditiously correct or remove all information found to be in error or data collected on a student or family in violation of this act. Any local education institution official or local education agency that refuses to provide information about the data of a student in a timely manner, or ignores a written request for student information from a parent or eligible student, is in violation of this act.

(1) A parent or eligible student is entitled to any information a local education agency or local education institution maintains on the student of the parent or the eligible student including, but not limited to, the curriculum and any programs implemented or curriculum used by the local education agency or in the local education institution.
(2) Any student information system data that is accessible online by an employee of a local education agency, local education institution, or student information system provider concerning a specific student, shall be viewable at all times by the parent or eligible student online or at the local education institution, during normal business hours, at no charge to the parent or eligible student. A copy or any record in the file shall be provided free of charge to the parent or eligible student, upon request.

(c) No student shall be required to complete any questionnaire, survey, or assessment regarding personal habits or attitudes or activities without prior informed parental written consent. The written consent shall include a complete copy of the questionnaire, survey, or assessment.

(d) No student may be denied services in a local education institution because his or her parent has exercised any right provided by this act.

(e) Redisclosure of personally identifiable student information to a third party is forbidden without the informed written consent of a parent.

(f)(1) No student may be arrested, seized, or searched on local education institution property without probable cause or proper warrant issued by a court of proper jurisdiction. The personal property of a student, while on local education institution property, may not be seized or searched without probable cause or proper warrant. For the
purposes of this subsection, personal property includes all of
the following:

a. Email accounts of the student, regardless of
whether the email account is provided by the local education
institution or controlled by a private company.

b. Digital correspondence created by a student on
his or her personal laptop or other electronic device.

c. Any document stored on a computer or other
electronic device of any type owned by the student.

d. Cell phone or home phone records on an electronic
device owned by a student.

e. Any online account in which the student is
required to use a username or email and password.

(2) A proper warrant or probable cause shall be
established before any information or data from any accounts
used by a student, or associated with the name of the student,
are searched or seized. A student locker may not be searched
without probable cause or proper warrant. A student may not be
questioned or interrogated by law enforcement without the
presence of either his or her attorney or his or her parent.

(g) A student may only be searched in a local
education institution without a warrant or probable cause if
the local education institution has established a security
check point or installed metal detectors at the entrance to
the local education institution. The search shall be a
minimally invasive pat down limited to searching only for
items that may impact safety and are prohibited by the local
education institution. Any item obtained during a search conducted pursuant to this subsection including, but not limited to, items that are illegal or in violation of local education institution rules, may be used as evidence in court or noted in an official local education institution record relating to the student, regardless of who performs the search. If a student objects to a body scan for medical or privacy reasons, a terry search shall be offered as an alternative to a full body search or metal detector scan.

Section 9. (a) A local education institution may not do any of the following:

(1) Require, request, or coerce a student or prospective student to disclose a username, password, or any other means of authentication, or provide access through the username or password, to a personal social media account.

(2) Require, request, or coerce a student or prospective student to access a personal social media account in the presence of an employee or volunteer of the local education institution including, but not limited to, a coach, teacher, or local education institution administrator, in a manner that enables the employee or volunteer to observe the contents of the account.

(3) Compel a student or prospective student to add anyone including, but not limited to, a coach, teacher, local education institution administrator, or other employee or volunteer, to his or her list of contacts associated with a personal social media account or require, request, or
otherwise coerce a student or applicant to change the settings that affect the ability of a third party to view the contents of a personal social media account.

(4) Take any action or threaten to take any action to discharge, discipline, prohibit from participating in curricular or extracurricular activities, or otherwise penalize a student for his or her refusal to disclose any information specified in subdivision (1), for refusal to take any action specified in subdivision (2), or for refusal to add a coach, teacher, local education institution administrator, or other employee or volunteer to his or her list of contacts associated with a personal social media account, or to change the settings that affect a third party’s ability to view the contents of a personal social media account as specified in subdivision (3).

(5) Fail or refuse to admit any prospective student as a result of the prospective student’s refusal to disclose any information specified in subdivision (1), for refusal to take any action specified in subdivision (2), or for refusal to add a coach, teacher, local education institution administrator, or other employee or volunteer to his or her list of contacts associated with a personal social media account, or to change the settings that affect a third party’s ability to view the contents of a personal social media account as specified in subdivision (3).

(b) Nothing in this act shall prevent a local education institution from doing any of the following:
(1) Accessing information about a student or prospective student that is publicly available.

(2) Complying with state and federal laws, rules, and regulations and the rules of self-regulatory organizations, where applicable.

(3) Prohibiting a student or prospective student from using a personal social media account for local education institution purposes.

(4) Prohibiting a student or prospective student from accessing or operating a personal social media account during local education institution hours or while on local education institution property.

(c) If a local education institution inadvertently receives the username, password, or other means of authentication that provides access to a personal social media account of an employee, applicant, student, or prospective student through the use of an otherwise lawful virus scan or firewall that monitors the network of the local education institution or devices provided by the local education institution, the local education institution is not liable for having the information, but may not use the information to access the personal social media account of the student or prospective student or share the information with any other person, and shall also delete the information immediately, or as soon as is reasonably practicable.

Section 10. (a) A student may not be denied access to any public educational service or grade advancement in the
public schools for failure to participate in or utilize any assessments, career counseling, workshops, psychological counseling session, or other activities that the parent of the student deems inappropriate or offensive.

(b) A parent or eligible student shall notify the local education institution in writing and name the program or programs they choose not to participate in pursuant to subsection (a).

(c) The parent or eligible student shall be offered a reasonable academic alternative.

Section 11. Evidence or information obtained or collected in violation of this act is not admissible in any civil or criminal trial or legal proceeding, disciplinary action, or administrative hearing except when used against the party who violated this act.

Section 12. (a) Each violation of this act by an organization, state agency, local education agency, or local education institution 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). Each violation of this act involving a different individual education record or a
different individual student shall be considered a separate 
vialation for purposes of civil penalties and reasonable 
attorney fees and other costs of litigation.

(b) The Attorney General or a local district 
attorney may enforce compliance with this act by investigation 
and subsequent commencement of a civil action, seek civil 
penalties for violations, and seek appropriate injunctive 
relief including, but not limited to, a prohibition against 
obtaining personally identifiable student information for an 
appropriate time period. In conducting an investigation and in 
maintaining a civil action, the Attorney General or district 
atorney may 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 Alabama Rules of Civil Procedure and state 

law.

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

Section 13. This act shall become effective on July 1, 2016, following its passage and approval by the Governor, or its otherwise becoming law.