

New law defines "biometric information" as the noninvasive electronic measurement and evaluation of any physical characteristics that are attributable to a single person, including fingerprint characteristics, eye characteristics, hand characteristics, vocal characteristics, facial characteristics, and any other physical characteristics used for the purpose of electronically identifying that person with a high degree of certainty.

Requires the governing authority of each public elementary and secondary school that collects biometric information from students to develop, adopt, and implement policies governing the collection and use of such information that, at a minimum:

1. Contains a full explanation of what type of biometric information will be collected, how it will be collected and stored, and the purposes for which such information will be used.
2. Requires written permission from the student's parent or other legal guardian, or the student if he or she is age 18 or older, prior to the collection of any biometric information. Requires a form created for the express purpose of obtaining the required permission. Further requires that the granting of permission shall not be included as a part of any form used for enrollment purposes or other form required by the school's governing authority for any other purpose.
3. Provides that any biometric information collected from a student shall be used only for identification or fraud prevention purposes.
4. Ensures that a student's biometric information shall not be disclosed to a third party without the written permission of the student's parent or other legal guardian, or the student if he or she is age 18 or older, unless the disclosure is required by court order.
5. Provides for the secure storage, transmission, and protection of all biometric information from unauthorized disclosure.
6. Encrypts student biometric information using an algorithmic process which transforms data into a form in which there is a low probability of assigning meaning to such information without use of a confidential process or key.
7. Ensures that the use of a student's biometric information is discontinued upon:
 - (a) The student's graduation or withdrawal from school.
 - (b) Receipt of a written request to discontinue use of such information from the student's parent or other legal guardian, or the student if he or she is age 18 or older.
8. Requires that all biometric information collected from a student be destroyed within 30 days after use of such information is discontinued.

Provides that a student shall not be refused or denied any services due to the failure to provide written consent.

Provides that the collection of student biometric information must comply with all applicable state and federal law and requirements, including the Federal Family Educational Rights Privacy Act of 1974.

Effective June 24, 2010.

(Adds R.S. 17:100.8)