Rule Overview

Date: November 18, 2026
Prepared By: Saraí Ortiz
Rule Citation: NMAC 6.11.3 – Student Data Privacy

Overview of Proposed Rule

Agency: Public Education Department
Rulemaking Action: New Rule
Date of Notice: October 20, 2026
Public Comment Period: October 20, 2026, to November 20, 2026
Rule's Purpose: The rule would require the Public Education Department (PED) and local education agencies (LEAs) to include specific privacy and security protections in contracts with kindergarten through 12th grade (K-12) education vendors that collect, store, and use student data.

Summary of NMAC 6.11.3 – Student Data Privacy

The proposed rule creates requirements for how PED, school districts, and charter schools manage student data in contracts with K-12 education companies or vendors that collect, store, or use student data. The rule would go into effect on April 1, 2027, if adopted.

Definitions. The proposed rule broadly defines student data using the Family Education Rights and Privacy Act (FERPA) framework including personally identifiable information from a student's education record such as names, addresses, test results, grades, health records, disciplinary records, socioeconomic information, and persistent unique identifiers. It also defines biometric information to include retina or iris scans, fingerprints, voiceprints, hand or face geometry scans, and any other biologically unique identifier used to identify a specific student. It also defines voiceprints as audio data processed to create a unique vocal signature capable of identifying a specific student. These proposed terms are significant to highlight as they are not currently defined in statute.

Consent Requirements. The rule would require school districts and charter schools provide parents with written notice in plain language explaining what biometric information will be collected, the specific purpose, how it will be stored, how long it will be retained, and how it will be destroyed before the student's biometric information can be collected. School districts and charter schools would be required to obtain parental consent for collection and storage of biometric information when required by law, but it would not be the default procedure.

Vendor Obligations. The rule would require PED and local education agencies' contracts with vendors to include the following:

- Restrict access to student data to authorized personnel with a legitimate need;
- Prohibit the use of student data for:
    - Targeted advertising directed students or parents;
    - The development of student profiles beyond what is necessary to deliver the contracted service; and
    - The transfer of student data to third parties unless those parties are bound by the same restrictions;
- Notify the contracting school or district within 48 hours of any unauthorized disclosure or data breach;
- Provide 60 days' written notice before any material change to a privacy policy or data-handling practice; and
- Ensure student records remain the property of and under the control of PED or the LEA.

Prohibition on Profiting from Student Data. The rule would prohibit vendors from selling, leasing, trading, or otherwise profiting from student data under any circumstances, including when the data has been anonymized, aggregated, disaggregated, or de-identified. This prohibition applies regardless of the form of the data after collection.

Disclosure Restrictions. The rule would prohibit vendors from disclosing, re-disclosing, or disseminating student data unless one of the following four conditions is satisfied:

- The parent consents in writing to the specific disclosure;
- Disclosure is required by state or federal law, or a valid court order;
- Disclosure is necessary to protect the safety of the student or others; or,
- Disclosure is otherwise permitted without consent under FERPA.

The rule would also require the vendor to notify the contracting LEA within 48 hours in the event of an unauthorized disclosure or breach. If an LEA is the contracting party, it must notify the parent within 72 hours of receiving that notice and notify PED within 48 hours. If PED is the contracting party, it must notify the impacted LEA within 48 hours, and the school must then notify the parent within 72 hours.

Procurement Requirements. Prior to signing a contract with a vendor, the rule would require vendors to provide school officials two documents: a plain-language data privacy impact assessment, and a security assessment conducted by a third-party auditor. The plain-language data privacy impact assessment would have to describe what data is collected, how it is used, where it is stored, who has access, and how it is protected. The security assessment would have to name the third-party auditor under a recognized framework such as SOC 2 Type II report, which is an independent audit of how well a vendor protects data over time, with results shared with the contracting department or LEA.

Contracts would also be required to include a termination clause permitting PED or the LEA to terminate a contract if the vendor violates a privacy requirement and does not cure the violation within 30 days of written notice, or if PED or the LEA does not agree with a material change to the vendor's privacy policy or data-handling practices.

Data Retention and Destruction. The rule would require vendors to destroy all student data within 30 days of the end of the collection period or at the end of the school year in which it was collected, whichever comes first. Vendors would also be required to destroy data within 30 days of written request from the LEA and provide written certification that destruction is complete. The rule would also prohibit the storage of student data outside the United States without prior written approval from the contracting LEA. Vendors would be required to maintain a data retention and destruction policy consistent with FERPA and make it available to the contracting party.

Impact

The proposed rule would address part of the student data privacy and procurement gap identified in a May 2026 LESC brief. It would require every contract between PED, school districts, or charter schools and a vendor handling student data to include a privacy impact assessment, a named third-party security assessment, a ban on profiting from student data, 30-day data destruction, breach notification, and termination rights. The rule does not specifically mention artificial intelligence (AI) education tools, but it would apply to AI tools that collect student data.

If approved, the rule would take effect on April 1, 2027, almost two years after PED's statewide implementation of Amira ISIP. Currently, Amira data practices store student audio for the duration of the state contract, but the proposed rule would require the destruction of voiceprints within 30 days or at the end of the collection period, whichever comes first. If Amira's voice processing creates a persistent vocal signature, the rule would require a standalone biometric notice to parents.

The rule could give parents limited protection and no clear enforcement mechanism. PED and local education agencies would be able to terminate a contract for a privacy violation, but the rule wouldn't create a private right of action, which could allow students or parents to sue vendors directly. Authority over consent would rest primarily with the department and LEAs. Schools would provide biometric notices, request data destruction,

approve vendor profiling and changes to vendor privacy terms, and receive breach notices before parents. The rule would require parental consent for biometric collection only when otherwise required by law, but it would not be the default standard, and it remains unclear which laws would require parental consent. The rule would also enable parents to provide written consent to certain vendor disclosures.

The proposed rule does not address tribal sovereignty or explicitly prohibit vendors from using student data to train AI models. Since the rule is proposed ahead of the 2027 legislative session, its final text could change, and lawmakers could consider legislation that aligns with it, or sets additional requirements.

TITLE 6 PRIMARY AND SECONDARY EDUCATION
CHAPTER 11 PUBLIC SCHOOL ADMINISTRATION - STUDENT RIGHTS AND RESPONSIBILITIES
PART 3 STUDENT DATA PRIVACY

6.11.3.1 ISSUING AGENCY: Public Education Department, herein after the department.
[6.11.3.1 NMAC - N, 4/1/2027]

6.11.3.2 SCOPE: This part applies to the department, local school districts, and charter schools with respect to student data that is collected, maintained, used, or disclosed in connection with public K-12 education in New Mexico, and to their contracts with vendors that collect, maintain, or use student data for K-12 school purposes.
[6.11.3.2 NMAC - N, 4/1/2027]

6.11.3.3 STATUTORY AUTHORITY: Sections 9-24-8, 22-2-1, 22-2-2, 22-2C NMSA 1978 and the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g and 34 CFR Part 99.
[6.11.3.3 NMAC - N, 4/1/2027]

6.11.3.4 DURATION: Permanent
[6.11.3.4 NMAC - N, 4/1/2027]

6.11.3.5 EFFECTIVE DATE: April 1, 2027, unless a later date is cited in the history note at the end of a section.
[6.11.3.5 NMAC - N, 4/1/2027]

6.11.3.6 OBJECTIVE: Establish requirements governing the department's, local school districts', and charter schools' collection, use, retention, and protection of student data, including biometric information, and to require that contracts between the department, local school districts, or charter schools and vendors include specific data privacy and security protections for students.
[6.11.3.6 NMAC - N, 4/1/2027]

6.11.3.7 DEFINITIONS:

A. "Biometric information" means retina or iris scan, fingerprint, voiceprint, scan of hand or face geometry, or any other biologically unique identifier used to identify a specific student, regardless of how it is captured, converted, stored, or shared.

B. "Destroy" or "destruction" means permanent deletion of student data and information from all systems, including any backups of that data or information.

C. "K-12 school purposes" means purposes that customarily take place at the direction of the department, a local school district, charter school, or teacher, or that aid in the administration of school activities, including instruction in the classroom, administrative activities, and collaboration among students, school personnel, or parents, or that are for the use and benefit of the school.

D. "Mandatory assessment" means a statewide summative or interim assessment, or a federally required assessment, that the department, local school district or charter school administers pursuant to the Assessment and Accountability Act, Article 22-2C NMSA 1978.

E. "Parent" includes a guardian or other person having custody and control of a school-age person;

F. "Profile" means the systematic collection, analysis, or scoring of a student's attributes, behaviors, or performance data beyond what is necessary to deliver the contracted educational service.

G. "Student data" means materials, in any media or format, that:

(1) contains personally identifiable information from a student's education record as defined under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g and 34 CFR Part 99;

(2) is created or provided by a student, or a student's parent or legal guardian, to a vendor in the course of the student's, parent's, or legal guardian's use of the vendor's site, service, or application for K-12 school purposes;

(3) is created or provided by an employee or agent of the department, a local school district, or charter school to a vendor; or

(4) is gathered by a vendor through operation of a site, service, or application and is descriptive of a student or otherwise identifies a student, including but not limited to information in the student's

education record, first and last name, home address, telephone number, email address, discipline records, test results, special education data, grades, evaluations, health records, biometric information, disability status, socioeconomic information, and persistent unique identifiers.

H. **"Vendor"** means an entity that enters into a contract that includes the collection or transfer of student data with the department, a local school district, or charter school.

I. **"Voiceprint"** means an audio recording, or data derived from an audio recording, that is processed to create a unique vocal signature capable of identifying a specific student by the student's vocal characteristics. "Voiceprint" does not include an audio or video recording of a student's speech that is not processed to create a persistent, student-identifying vocal signature usable outside the purposes of the assessment or program.
[6.11.3.7 NMAC - N, 4/1/2027]

6.11.3.8 CONSENT REQUIREMENTS FOR BIOMETRIC INFORMATION: Before collecting any biometric information from a student, a local school district or charter school shall:

A. Provide the student's parent or legal guardian with a written, standalone notice that explains in plain language what biometric information will be collected, the specific purpose for collecting it, how it will be stored, how long it will be retained, and how it will be destroyed.

B. A local school district or charter school shall obtain parental consent for collection and storage of biometric information when otherwise required by law.
[6.11.3.8 NMAC - N, 4/1/2027]

6.11.3.9 VENDOR OBLIGATIONS FOR STUDENT DATA: A contract between a vendor and the department, a local school district, or a charter school shall require that the vendor:

A. Restrict access to student data exclusively to authorized personnel who have a legitimate need to know and access such data solely to perform the services specified in the contract.

B. Not use student data to engage in targeted advertising directed at students or their parents.

C. Not use student data to create a profile about a student, except as necessary to deliver the contracted educational service or as the contracting local school district, charter school, or department has approved in writing. A vendor may not add "profiling" to its stated uses of student data without prior written approval from the contracting local school district, charter school, or department, and may only do so as necessary to deliver the contracted educational service or as permitted by the contracting local school district, charter school, or department.

D. Not sell, lease, trade, or otherwise transfer student data to any third party, except as needed to provide the contracted educational service, and only where the third party is bound by the same restrictions.

E. Not retain student data beyond the term of the contract with the school or district, unless the school or district requests otherwise in writing.

F. Destroy student data within 30 days of a school's or district's written request for destruction or within 30 days after the termination of the contract.

G. Implement and maintain reasonable security procedures and practices appropriate to the sensitivity of the student data.

H. Ensure that student records remain the property of and under the control of the school, local school district, or the department, not the vendor.

I. Provide at least 60 days' written notice to the contracting local school district, charter school, or department, and obtain written acknowledgment, before any material change to a privacy policy, terms of service, or data-handling practice that affects student data takes effect. Such a change made without this notice and acknowledgment shall be void and unenforceable.
[6.11.3.9 NMAC - N, 4/1/2027]

6.11.3.10 DATA RETENTION AND DESTRUCTION: A contract between a vendor and the department, a local school district, or a charter school shall require that the vendor:

A. Develop and make available to the contracting local school district, charter school, or department a written policy establishing a retention schedule and guidelines for destroying student data consistent with FERPA, 34 CFR Sections 99.35.

B. Transfer student data to the school or school district when retention is required by applicable state or federal law or school district policies.

C. Destroy all student data within 30 days of the end of the collection period, or at the end of the school year in which it was collected, whichever comes first.

D. Certify in writing to the school district or charter school that destruction has been completed within the required timeline.

E. Never store student data outside of the United States without prior written approval from the school district or charter school.

[6.11.3.10 NMAC - N, 4/1/2027]

6.11.3.11 PROHIBITION ON PROFITING FROM STUDENT DATA: A contract between a vendor and the department, a local school district, or a charter school shall provide that the vendor may not sell, lease, trade, or otherwise profit from a student's data, regardless of whether the data is anonymized, aggregated, disaggregated, or de-identified.

[6.11.3.11 NMAC - N, 4/1/2027]

6.11.3.12 DISCLOSURE RESTRICTIONS: A contract between the department, a local school district, or a charter school and a vendor shall provide that:

A. No vendor may disclose, redisclose, or otherwise disseminate student data unless:

(1) The student's parent or legal guardian consents in writing to the specific disclosure;

(2) The disclosure is required by state or federal law, or pursuant to a valid court order;

(3) The disclosure is necessary to protect the safety of the student or others; or

(4) The disclosure is otherwise permitted without consent under FERPA, 20 U.S.C. Section 1232g and 34 CFR Part 99.

B. When a disclosure is made that is not authorized under Subsection A of this section, or a breach or unauthorized access is discovered:

(1) The vendor shall notify the contracting local school district, charter school, or department within 48 hours.

(2) When a local school district or charter school is the contracting entity, the local school district or charter school shall notify the student's parent or legal guardian within 72 hours of receiving that notice. The local school district or charter school shall notify the department within 48 hours of receiving notice of unauthorized disclosure from the vendor.

(3) When the department is the contracting entity, the department shall notify the applicable local school district or charter school within 48 hours of receiving notice of unauthorized disclosure from the vendor, and the local school district or charter school shall provide the required notification to the student's parent or legal guardian within 72 hours of receiving notice from the department.

C. Where a vendor shares de-identified, anonymized, or aggregate data derived from student data, the vendor shall take reasonable measures to ensure the data cannot be re-associated with any student or household and shall contractually prohibit recipients from attempting re-identification.

[6.11.3.12 NMAC - N, 4/1/2027]

6.11.3.13 PROCUREMENT REQUIREMENTS: A contract between a vendor and the department, a local school district, or a charter school shall, as a condition of the contract:

A. Require the vendor to provide, before the contract is signed, a plain-language data privacy impact assessment that describes what data is collected, how it is used, where it is stored, who has access, and how it is protected.

B. Require the vendor to provide a security assessment determined by the contracting local school district, charter school, or department. The security assessment may be satisfied by either an independent third-party audit or a vendor security assessment conducted under a recognized framework, such as a SOC 2 Type II report from a named auditing firm, with results shared with the contracting local school district or charter school and department. A vendor-asserted certification that does not name the auditing firm or provide the underlying report shall not satisfy this requirement.

C. Include a provision under which the department or the contracting local school district or charter school may declare the contract void upon written notice to the vendor, following a 30-day opportunity-to-cure period, if the vendor is found to have materially violated a privacy requirement of the contract that the vendor did not cure within that period.

D. Require that any material change to the vendor's privacy policy, terms of service, or data-handling practices be submitted to the contracting local school district, charter school, or the department for review at least 60 days before taking effect, and that such changes be approved in writing by the contracting local school district,

charter school, or the department before they become effective. Failure of the parties to agree on a material change to the vendor's privacy policy shall explicitly constitute grounds for termination of the underlying contract by the local school district, charter school, or the department.
[6.11.3.13 NMAC - N, 4/1/2027]

6.11.3.14 SEVERABILITY: In the event that any one or more of the sections of this rule, in whole or in part, should be held to be invalid, illegal, or unenforceable in any respect, the validity, legality, and enforceability of the remaining sections of this rule shall not in any way be affected or impaired.
[6.11.3.14 NMAC - N, 4/1/2027]

History of 6.11.3 NMAC: [RESERVED]