STATE LEVEL STUDENT DATA COLLECTION AND PROTECTION

Nevada Department of Education
http://www.doe.nv.gov/

The Nevada Department of Education (NDE) is committed to using accurate student and program information to improve student performance and allow leaders, administrators, teachers, students and parents to make informed educational decisions. Federal and state law requires the Department to collect student level information for student, school and district performance reporting, evaluation of educational programs and allocation of state funding. The Family Educational Rights and Privacy Act (FERPA) establish baseline parameters for what is permissible when sharing student information. The Nevada Department of Education adheres to all FERPA and State regulations involving student privacy to protect the privacy of every student and ensure the confidentiality and security of all data collected and managed.

What student information does NDE collect?

Data collection categories for all students:
- Student demographics
    - Name
    - Birthdate
    - Race/Ethnicity
    - Gender
    - Address
    - Parent contact information
- Enrollment
    - State Unique Identifier (UID)
    - School
    - District
    - Grade
    - Entry/Exit date/type
    - Courses completed

- Program Participation
    - Title I
    - Special Education/Gifted
        - Disability/Gifted type
        - Services received
        - Select Individual Education Plan (IEP) data
    - Free or reduced lunch (FRL)
    - English language learner (ELL)
        - Primary language
        - English language proficiency level
    - Migrant student
- Early childhood
    - Enrollment status in State programs
- Concurrent Enrollment
    - Participating institution
- Career and Technical Education (CTE)
    - Program participation
    - Program assessment results

State Assessment for students in assessed grades:
- Criterion Reference Tests (CRT)
- High School Proficiency Exams (HSPE)
- Alternate special needs assessments

Why does NDE collect student information?

- Federal or State Law

Where is the information stored?

- All state data is stored at the secure State Technology Facility
- Secure, encrypted back-up copies of the data are retained through a Service Level Agreement between NDE and the State Enterprise Information Technology Agency

How is student information used?

Individual student data uses:
- Administering state assessments
- Calculating individual student growth
- Determining scholarship eligibility (Millennium, Gear-up)

Aggregated student data uses:
- Allocation of state funding
- School and District performance reports
- Program evaluation and measurement
- School and District improvement plans
- Federal reporting/funding
- Public reporting (Nevada Report Card, Nevada Growth Model)
- Nevada post-secondary enrollment and remediation feedback

How is information safeguarded?

- Access control
  - Strong passwords/90 day exp.
  - Local access management
  - Access logging
  - Vulnerability testing
  - All staff security awareness training
- Encryption
  - Use of state assigned Unique ID to isolate student data from student names
  - Multi-level database encryption

- Secure Transit
  - Secure File Transfer Protocol (SFTP)
  - Hypertext Transfer Protocol with Secure Socket Layer (HTTPS)
- Physical security
  - Controlled building and Data Center access
  - Video surveillance
  - 24 hour staff on-site
- Suppression of small n-sizes for aggregated student data reports

Who has access to student data?

- Authorized and authenticated NDE officials and information technology personnel
- Authorized and authenticated District and School personnel
- Contracted vendors with signed privacy obligations for specified applications
- Parents and students may access this data through their local district

How NDE meets or exceeds Federal and State privacy laws

- Formal information security policy
- District guidance for student data security and privacy policies
- Policy review and revision by national experts and information security advisors
- Data governance committee to determine internal accountability for student data
- Data breech notification and liability clauses in vendor contracts and agreements