## Overview

The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974 that protects the privacy of student education records. It applies to all educational institutions and agencies that receive funds from the U.S. Department of Education.

## Who Must Comply

All School district staff and employees within the State Department of Education and Early Development (DEED) who handle, review, or have access to student education records must comply with [FERPA regulations](https://studentprivacy.ed.gov/ferpa).

## Key Provisions of FERPA

- Right to Inspect and Review Records: Parents or eligible students (18+ or attending postsecondary institutions) have the right to review education records maintained by the school.

- Right to Request Amendment: If records are inaccurate or misleading, parents or eligible students can request corrections.

- Right to Consent to Disclosure: Schools must generally have written permission before releasing student information, except under specific permitted exceptions.

- Right to File a Complaint: Complaints about FERPA violations can be submitted to the U.S. Department of Education.

## What Are Education Records?

Records that are directly related to a student and maintained by an educational institution or party acting on its behalf. This includes grades, transcripts, class lists, student schedules, and health records (if maintained by the school).

## Directory Information

FERPA allows schools to disclose, without consent, 'directory information' such as name, address, telephone number, date of birth, honors, and attendance dates. However, parents and eligible students must be given the opportunity to opt out of such disclosures.

## FERPA Exceptions Relevant to State/District Staff

- Legitimate Educational Interest: Employees may access student records only if their job responsibilities require it.

- Audit or Evaluation: DEED may access records to audit or evaluate federally or state-supported education programs.

- Studies for or on behalf of the School: Information may be shared to conduct studies to improve instruction, provided data privacy safeguards are in place.

- Judicial Orders or Subpoenas: Records may be released to comply with a lawfully issued subpoena or court order (with appropriate notification to the student/parent unless prohibited).

## Best Practices for School Employees

- Only Access What You Need: Access only the data necessary to fulfill your job duties.

- Secure Data: Use secure systems for storing and transmitting student data. Avoid using personal devices or unsecured email.

- Training: Participate in regular FERPA and data privacy training.

- Breach Protocol: Report any suspected or actual data breach immediately according to Local policy.

- Consult Before Sharing: Always verify if disclosure is permitted before sharing any student information, even internally.

## FERPA Contact and Training

- U.S. Department of Education, Family Policy Compliance Office: <https://studentprivacy.ed.gov>

- FERPA federal web site: <https://studentprivacy.ed.gov/ferpa>

- FERPA 101 Training for school districts from the US Department of Education: <https://studentprivacy.ed.gov/training/ferpa-101-local-education-agencies>

- FERPA 201 Training for Data Sharing requirements and processes from the US Department of Education: <https://studentprivacy.ed.gov/training/ferpa-201-data-sharing-under-ferpa>

- Parents Rights under FERPA Document from the US Department of Education: <https://studentprivacy.ed.gov/sites/default/files/resource_document/file/A%20parent%20guide%20to%20ferpa_508.pdf>