



Making FERPA as Simple as **Green, Yellow, or Red**

Student information helps educators, students, parents, and policymakers make informed decisions and provide tailored education to ensure each student is on track to succeed. Data use can be transformative, and protecting student privacy is an essential component of effective data use.

The foundational federal law on student privacy, the Family Educational Rights and Privacy Act (FERPA), establishes student privacy rights by restricting with whom and under what circumstances schools may share students' personally identifiable information. This tool summarizes some of the main provisions of FERPA, and identifies when students' personally identifiable information may be shared under the law. However, this tool should be used as a guide to help you understand when you need to take a closer look at the law or consult an expert. It should not be considered a comprehensive review of FERPA-authorized disclosures and should not be considered a substitute for appropriate legal counsel.



For more information, check out these sections of FERPA:

§99.30 Under what conditions is prior consent required to disclose information?

§99.31 Under what conditions is prior consent not required to disclose information?

View the full text of the law at http://bit.ly/FERPA_law.

FERPA RULES OF THE ROAD

Stop

NO ONE
Can **sell** student education record data.

AUTHORIZED THIRD PARTIES
Can't use personally identifiable information from educational records **to market to kids and families.**

EMPLOYERS
Can't be given a student's personally identifiable information, unless applicants or their parents (if applicants are under age 18) give consent.

SCHOOL OFFICIALS & AUTHORIZED THIRD PARTIES
Must have a **legitimate educational need** for student data before they can view them.

AUTHORIZED THIRD PARTIES
Can use data **only for the original purpose for which the data were shared**, and each third party is **under the direct control of either the school district or the state education agency.**

Slow Down

RECIPIENTS
Must maintain strict data use and security requirements where applicable. This includes **using data only for the purposes for which they were disclosed** and **destroying the data when no longer needed** for the specified use.

ANOTHER SCHOOL
Can receive data if **the student seeks or intends to enroll in that school**, including a postsecondary institution.

PARENTS
Can access **their child's education data** if the child is younger than 18 and not enrolled in postsecondary education.

SCHOLARSHIP & FINANCIAL AID PROVIDERS
Can receive data when the **student has applied for or received financial aid** from that entity.

STUDENT'S TEACHER
Can access the **student's data** to meet educational needs.

HEALTH & SAFETY
Student data can be shared for reasons of **health and safety** in certain emergencies.

Go



DISCLOSURE TO PARENTS: FERPA requires that the parent of a student who is younger than 18 and not enrolled in postsecondary education be able to review his or her child's records.

DISCLOSURE WITH PARENTAL CONSENT: FERPA permits a school to disclose student record data if a parent provides written consent.

DISCLOSURE WITHOUT PARENTAL CONSENT: FERPA establishes a limited number of ways in which student record data can be disclosed without prior parental consent. These disclosures include the following:

- Disclosure is permitted to **school officials, including teachers, who have legitimate educational interests** in the data.
- FERPA permits schools to disclose **directory information**, which is personally identifiable information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed, such as name, address, name of parent, etc. Directory information may not include a student's Social Security number or identification number. Schools that elect to disclose directory information must notify parents of their policy to do so, and parents have the right to opt out of these disclosures.
- Data can be shared with officials of **another school, school system, or institution of postsecondary education where the student seeks or intends to enroll or where the student is already enrolled** so long as the disclosure is for purposes related to the student's enrollment or transfer.
- The disclosure is in connection with **financial aid for which the student has applied or which the student has received**.
- The disclosure is in connection with a **health or safety emergency**, under certain conditions.

No Detours for Parents to Access Education Records

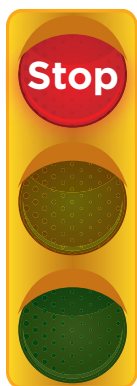
FERPA provides parents with the right to access and review their children's education records and to challenge information contained therein.

Schools cannot charge parents for access to or copies of their child's education record if the cost effectively prevents the parent from exercising his or her right to review it.



DISCLOSURE WITHOUT PARENTAL CONSENT: FERPA establishes a limited number of ways in which student data can be disclosed without prior parental consent. These disclosures include the following:

- Personally identifiable information can be shared with **third parties that provide outsourced services to the schools, if access to the data is necessary to provide that service.** For example, schools may use a contractor to conduct school assessments, provide student support services, or maintain the school's database. These parties must remain under the direct control of the school with respect to the use and maintenance of data and can use the data only for the purpose for which they were disclosed.
- Data can be shared with **authorized representatives of certain state or local education officials to audit or evaluate a state- or federally supported education program or to conduct a compliance or enforcement activity** under related federal laws. Authorized representatives must safeguard personally identifiable information and must destroy the information once they are finished using it for its intended purpose. §99.31 (a)
- Personally identifiable information can be shared with **researchers who conduct studies for or on behalf of schools and school districts** to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction, subject to a required written agreement between the education agency and the research organization. Personally identifiable information can be shared only with researchers with a legitimate interest in the data and **cannot be released publicly.** Data may be used only for the purpose for which they were disclosed and must be destroyed when no longer needed for the study.



DISCLOSURE NOT ALLOWED: Most other disclosures of students' personally identifiable information are not permitted under FERPA.

- This means that under FERPA, schools **may not share student data for commercial purposes or marketing without parental consent.**
- FERPA also **does not permit the sharing of student data to make decisions regarding a student's (or former student's) employment** unless the job applicant (or parent) consents to a disclosure.



The Data Quality Campaign (DQC) is a nonprofit, nonpartisan, national advocacy organization committed to realizing an education system in which all stakeholders—from parents to policymakers—are empowered with high-quality data from the early childhood, K-12, postsecondary, and workforce systems. To achieve this vision, DQC supports policymakers and other key leaders to promote effective data use to ensure students graduate from high school prepared for success in college and the workplace.

For more information, visit www.dataqualitycampaign.org or email info@dataqualitycampaign.org.