



Q & A: Protecting the Privacy of Student Educational Records and Personally Identifiable Information

The Minnesota Department of Education (MDE) Division of Compliance and Assistance developed this document to assist school districts who have raised questions about protecting the privacy of student educational records. The intention of this document is to provide helpful, general information to the public. It does not constitute legal advice nor is it a substitute for consulting with a licensed attorney. The information below should not be relied upon as a comprehensive or definitive response to your specific legal situation. This document may not include a complete rendition of applicable state and federal law.

Question 1: What state and federal laws protect the privacy of student educational records and information?

Answer: The Minnesota Government Data Practices Act, Chapter 13 of Minnesota Statutes, is the state law that protects the privacy of student educational records. The Federal Educational Rights Privacy Act (FERPA) is the federal law that protects personally identifiable information included in student educational records.

Authority: Minnesota Government Data Practices Act, Chapter 13 of Minnesota Statutes and the Federal Educational Rights Privacy Act, 34 C.F.R. §§ 99.1-99.67

Question 2: Is educational data private or public data?

Answer: Educational data is private data under state law. Minnesota Statutes, section 13.32, defines educational data broadly as any data on an individual maintained by a public educational agency or institution which relates to a student. Generally, private educational data cannot be disclosed to a third party, unless a statutory exception applies or appropriate consent has been given by the parent or eligible student (18 or older). Minn. Stat. § 13.32, Subd. 3.

FERPA defines education records as any record that directly relates to a student and is maintained by an educational agency or institution or by a party acting for the agency or institution. Personally identifiable information includes a student's name, social security number, student number, or other information linked to a specific student that would allow a person in the school community to identify the student. 34 C.F.R. § 99.3. Generally, under FERPA, personally identifiable information cannot be disclosed without written consent from a parent or an eligible student. 34 C.F.R. §§ 99.30-31.

Authority: Minn. Stat. § 13.32, Subd. 3; 34 C.F.R. §§ 99.3 and 99.30-31

Question 3: Can information from a student's private educational record be disclosed to school officials without consent?

Answer: FERPA provides that personally identifiable information from a student's education record *can* be disclosed without consent if an exception applies. 34 C.F.R. § 99.30. Under one such exception, an educational agency or institution may disclose personally identifiable information from a student's education record without consent if the disclosure is made to a school official, including teachers and paraprofessionals, within the agency or institution that the agency or institution has determined to have a legitimate educational interest to access to data. 34 C.F.R. § 99.31(a)(1)(i)(A).

Authority: 34 C.F.R. §§ 99.30 and 99.31(a)(1)(i)(A)

Question 4: Can private educational data or personally identifiable information be disclosed to any school official simply because they are school or district staff?

Answer: No. According to the Family Policy Compliance Office (FPCO) that enforces FERPA, it is a violation of FERPA for a school to disclose personally identifiable information in a student's educational record to an individual “solely on the basis that the individual is a school official if it does not also determine that the school official has a legitimate educational interest.” Thus, a school must determine that a school official has a legitimate educational interest in accessing a student's educational record in order to comply with FERPA requirements.

Authority: 34 C.F.R. § 99.31(a)(1)(ii), cmts. at 73 FR 74817 (2008).

Question 5: How does a school or district determine who has a legitimate educational interest?

Answer: FERPA states that “an educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those educational records in which they have legitimate educational interests. An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to educational records is effective and that it remains in compliance with the legitimate educational interest requirement.” 34 C.F.R. § 99.31(a)(1)(B)(3)(ii). The FPCO states that a school should use a “reasonable methods” approach to determine the appropriate physical, technological, and administrative controls to prevent unauthorized access to education records. These regulations are intended to ensure that access to educational records by school officials, including teachers and paraprofessionals, is limited to circumstances in which the school official possesses a legitimate educational interest in the record.

Authority: 34 C.F.R. § 99.31(a)(1)(B)(3)(ii); 34 C.F.R. § 99.31(a)(1)(ii), cmts. at 73 FR 74817 (2008)

Minnesota Department of Education
1500 Highway 36 West, MN 55113-4266 651-582-8200 TTY: 651-582-8201

education.state.mn.us

Question 6: What can I do to prevent unintentional disclosure of private educational data?

Answer: As stated above, teachers and paraprofessionals can discuss student information and pass that information along to other school officials if the school has determined that each recipient of the information has a legitimate educational interest in knowing or accessing the student's private educational information or if the parent or eligible student has provided consent. As a best practice, school professionals who have a legitimate educational interest in sharing private student educational data should not discuss student information in community areas such as hallways, lounges, and parking lots in order to prevent the unauthorized disclosure of private student data. Furthermore, privacy of information can often not be guaranteed when using emailing and faxing as communication methods. School staff should carefully weigh the risks of the communication methods they use. Overall, school staff should refrain from discussing personal student information in public areas and be aware of the security risks of the communication methods used when sharing private student data, such as in emails or faxes.