



OPI Employee Confidentiality Agreement

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. The law applies to all schools receiving certain funds from the U.S. Department of Education. FERPA allows parents certain rights with respect to access to and confidentiality of their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.

OPI employees must make reasonable efforts to provide for the security of confidential information. Violation of the provisions of FERPA may result disciplinary action against the employee, up to and including termination.

To help ensure the security of confidential student information and data:

1. An employee will report to the employee's supervisor any actual or suspected unauthorized access to, or release of confidential student data to the employee's supervisor. (The supervisor will review MCA §§ 2-6-1501 through 1503, to ensure that, in the event of a breach of confidential data, all necessary steps are taken and notifications made.)
2. An employee will be granted access to only the level of information required by his or her job duties.
3. An employee will provide confidential information only to persons who are authorized to receive the information.
4. To ensure confidential information is not visible to unauthorized persons, each employee must:
 - i. clear information from the computer screen when not being used or minimizing applications when away from the work space or when approached by an unauthorized person
 - ii. protect visibility of reports and computer monitors when displaying confidential information;
 - iii. lock or shutdown workstations when left unattended;
 - iv. store electronic data in a password protected, secure location only accessible by the authorized entity;
 - v. encrypt email containing PII, or use the file transfer process set up in ePass. Instruction for using ePass can be found at <https://app.mt.gov/epass/portal/instruct.html>; and
 - vi. store reports, forms and correspondence containing confidential student information in a locked drawer or file cabinet when away from the work place.
5. Confidential information should not be emailed or faxed. If confidential information is received by email, it should be deleted.
6. Verbal conversations regarding confidential information must only be with authorized personnel, should use as little identifying information as possible, and be conducted in a manner and setting that minimizes the amount of the conversation that can be overheard by other individuals.

For answers to questions concerning this agreement, contact your supervisor or the Data Collection Bureau Chief in the Measurement and Accountability Division.

My signature indicates that I have reviewed this document, the OPI Student Records Confidentiality Policy, and security video(s). I understand the requirements regarding confidentiality contained in each, and I agree to abide by the requirements.

Printed Name

Signature

Date

Return the completed form to the OPI Security Officer.