Office of Public Instruction Policy

Policy: OPI 7.2.01	Subject: STUDENT RECORDS CONFIDENTIALITY
Chapter 7: INFORMATION TECHNOLOGY	Page 1 of 8 and Resource A—OPI Employee AIM Access Request; Resource B—OPI Employee Confidentiality Agreement; Resource C—OPI Data Tiers for Release of Data; Resource D—OPI Cell Suppression Flow Chart; Resource E—OPI Affidavit of Non-Release; Resource F—Contractor's Employee or Contractor Nondisclosure Statement; Resource G—Researcher-FERPA Memorandum of Understanding; Resource H—FERPA Memorandum of Understanding Audit-Evaluation Exception
Owner: MEASUREMENT AND ACCOUNTABILITY DIVISION ADMINISTRATOR	Effective Date: September 15, 2015 Revised: October 5, 2016

I. POLICY

This policy establishes procedures and responsibilities under federal and state laws governing the access, use, and dissemination of confidential, sensitive, and/or restricted student information by the Montana Office of Public Instruction (OPI).

II. APPLICABILITY

These policies and procedures apply to all OPI departments, divisions, programs, and employees.

III. DEFINITIONS

Agent of the OPI is an entity that contracts with the OPI or with the U.S. Department of Education with written authorization to analyze confidential data or to provide some other service involving confidential data.

AIM (Achievement in Montana) is Montana's statewide student information system.

Covered Entities are local education agencies, nonpublic accredited schools, state-operated schools, and residential treatment centers.

Data Breach is defined in Montana Code Annotated (MCA) 2-6-1501.

Data Privacy and Security Committee is the committee whose members are the OPI Senior Office Administrator, chief legal counsel, and administrator for the OPI Measurement and Accountability Division (M&A).

Directory Information means information, as defined in FERPA 20 U.S.C. §1232g(a)(5)(A), 34 CFR §99.3, collected by the local education agency pertaining to an individual student that would not generally be considered harmful or an invasion of privacy if disclosed.

Disclosure means to permit access to, or the release, transfer, or other communication of, education records, or a student's personally identifiable information contained in those records, to any party, by any means, including oral, written, or electronic means.

Education Records means records, files, documents, and other materials recorded in any way that contain information directly related to a student and are maintained by an education agency or institution or by a person acting for such agency or institution. See FERPA 20 U.S.C. §1232g(a)(4).

FERPA is the acronym for the Family Educational Rights and Privacy Act, 34 CFR, Part 99, http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html.

Local Education Agency (LEA) means the local school district board of trustees recognized as the administrative agency for a public elementary or secondary school. For the purpose of this policy, references to LEAs include the State of Montana special education cooperatives.

OPI Employee is any person employed by the OPI, including full-time, part-time, seasonal, permanent staff, temporary staff, and short-term workers. Honoraria recipients and independent contractors are not employees.

Personally Identifiable Information (PII) means education records which pertain to an individual student and may easily lead to that student's identity with reasonable certainty. FERPA regulations list personally identifiable student information as including, but not limited to, the following:

- the student's name;
- the name of the student's parent or other family member;
- the address of the student or student's family;
- a personal identifier, such as a social security number or student number;
- a list of personal characteristics that would make the student's identity easily traceable; or
- other information that would make the student's identity easily traceable.

IV. OFFICE OF PUBLIC INSTRUCTION PROCEDURES

A. Mandatory Training

Training regarding confidentiality of student records is mandatory for all OPI employees. Training consists of reading this policy and watching the OPI Student Records Confidentiality and Security presentation on the OPI website.

B. General Requirements for Disclosure of Student Information

1. All information about Montana individual students submitted to the OPI is considered an education record protected by FERPA, with strict limitations regarding who may see or have access to the records or data. No data handled by the OPI is considered to be directory information.

2. The Information Technology Services Division and the M&A at the OPI are primarily responsible for releasing student-level data once the appropriate form has been signed.

3. The OPI Security Officer and AIM Unit Manager will maintain copies of all signed and approved access request forms, confidentiality agreements, and affidavits of non-release. Any rights that need to be assigned to employees or agents of the OPI will be assigned by either the OPI Security Officer or the AIM Unit Manager.

4. The OPI will disclose education records, without consent, to the parties listed below under the following conditions:
   a. other schools in order to facilitate school enrollment when a student is transferring;
   b. specified officials for audit or evaluation purposes;
   c. organizations authorized by a school to conduct certain studies for or on behalf of the school;
   d. appropriate officials in cases of health and safety emergencies; and
   e. Department of Justice driver's license staff for traffic education course completion and traffic education learner licenses issued by approved instructors.

5. The OPI may disclose, without consent, student information in aggregate form as described in the Resource D—Cell Suppression Flow Chart.

C. Obtaining Access to Confidential Student Information

1. OPI Employees.

    a. Access to PII shall be granted only to personnel who are authorized by the OPI on a need-to-know basis in the performance of their duties. Access to confidential information carries with it the responsibility to protect the data from further disclosure.

    b. OPI employees who need to access PII in AIM must complete and submit an Resource A—OPI Employee AIM Access Request Form maintained by the AIM Unit Manager and the Resource B—OPI Employee Confidentiality Agreement maintained by the OPI Security Officer. The division administrator of the person requesting access to confidential information must sign the form that indicates the person needs access to this information in the performance of his or her assigned duties and responsibilities. The OPI AIM Staff will disable AIM user accounts after 90 days of inactivity.

    c. OPI employees who do not need access to AIM but who need to use PII in the course of their job duties must sign the Resource B—OPI Employee Confidentiality Agreement.

    d. Authorization to access or receive PII must be evaluated annually and reapproved as appropriate to ensure access to the data is still required. The OPI Security Officer will coordinate the annual evaluation.

    e. OPI employees may not access confidential student information for any personal reason or purpose.

2. Non-OPI Staff.

    a. Agent of the OPI—Data collection and analysis for the purpose of fulfilling the objectives of a contract with an agent of the OPI may not be released to any third party, including contractor's employees, for any purpose without written permission of the OPI.
        i. The OPI liaison responsible for contracting with an agent of the OPI to provide a service involving confidential data is also responsible for securing an Resource F—Contractor's Employee or Contractor Nondisclosure Statement with the agent of the OPI to ensure strict confidentiality of the confidential data or PII with the original contract.
        ii. When an agent of the OPI contracts with another entity (third party) to provide a service involving confidential

data, these entities are considered agents for data access purposes. The OPI employee responsible for contracting with an agent of the OPI must ensure that the third party enters a Resource F—Contractor's Employee or Contractor Nondisclosure Statement and complies with the same conditions applicable to any agent of the OPI.

iii. Prior to gaining access to PII, an agent of the OPI must sign and have approved the appropriate data access request form. Authorization must be evaluated annually and reapproved as appropriate.

iv. The OPI employee responsible for releasing confidential data must ensure that a Resource E: OPI Affidavit of Non-Release has been signed prior to the data being released and filed with the OPI Security Officer.

b. Researchers—The Data Privacy and Security Committee is responsible for reviewing and approving requests by researchers for confidential data or PII.

i. The release of data to researchers outside the agency is considered a loan of data. Recipients of the data do not have ownership of the data.

ii. Following approval by the Data Privacy and Security Committee, the administrator of M&A is responsible for contracting with any researcher approved to analyze confidential data or PII to ensure strict confidentiality, including that any PII shared with researchers must be destroyed when the data is no longer needed for the purposes for which it was requested. See the Resource G—Researcher-FERPA Memorandum of Understanding.

c. Auditors and Evaluators—The OPI liaison responsible for contracting with an entity to analyze confidential data, or to provide some other service involving confidential data, must ensure that the terms of the contract comply with the same conditions applicable to the OPI liaison and that a Resource E—OPI Affidavit of Non-Release or the Resource H—FERPA Memorandum of Understanding Audit-Evaluation Exception has been signed by the contractor and filed with the original contract.

D. Protecting Student Data

1. All agency employees, agents of the OPI, researchers, and other entities with access to confidential student PII are responsible for protecting the data.
2. Measures to protect confidential student PII include:

a. protect visibility of reports and computer monitors when displaying and working with confidential information;

b. lock or shutdown workstations when left unattended;

c. store electronic data in a password protected, secure location only accessible by the authorized entity;

d. protect physical data (including hard copies of reports, storage media, notes, and backups) from unauthorized persons and secure when not in use;

e. change data to guarantee anonymity and omit or mask counts of five or fewer if reports containing any confidential student information are used in meetings or presentations or presented to anyone without authorized access to the information;

f. shred paper reports and destroy electronic files in accordance with the Montana Secretary of State's Local Government Retention and Disposition Schedule when no longer needed;

g. do not fax PII;

h. stamp or otherwise mark all reports, CDs, or any other media containing PII (including protective envelopes) as confidential prior to being released outside the agency;

i. 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

j. permanently delete any email received containing unencrypted PII and reply to the sender with instructions on acceptable methods for transmitting PII.

E. Cell Suppression Flow Chart

1. No cells of data that contain five or fewer students in a group will be publicly reported or released and must be suppressed to protect the identity of the students.

2. Exceptions to this policy are:

   a. total school enrollment counts and school enrollment counts disaggregated by grade level, and/or gender are reportable for any count;

   b. providing data to a school official with a legitimate education interest that includes only data from that school district and its students are reportable for any count;

   c. providing data to an OPI employee with a legitimate educational interest related to that employee's program are reportable for any count; and

   d. if the data are for special education disability counts, the counts are suppressed if they are less than 10.

3. The OPI will report student counts to the U.S. Department of Education and other federal agencies as required by federal laws and regulations governing education grant programs. The OPI will not suppress data reported to federal agencies. These federal agencies are subject to FERPA policy and regulations regarding the disclosure of confidential student information.
4. The OPI will suppress data in the form of percentages when the percentage is 100 percent for any student demographic category. Percentages will also be suppressed whenever the cell count that makes up the percent is five or fewer.
5. If cell counts or percentages are broken into separate categories and the total is listed (i.e., separated by proficiency levels on a test and the total number of students tested) then additional rules apply to suppression. If only one cell is suppressed because it contains five or fewer, then a second cell must also be suppressed, even if it is not five or fewer.
6. If all suppressed cells within a group have counts of zero, then one additional cell must be suppressed. The rules in this paragraph only apply if the total number of the group is listed, with the reasoning being an exact cell count of five or fewer should not be able to be found from the other data being presented.
7. Any given numeric or nonnumeric characteristics, variable values, or data element shared by five or fewer students in individual or aggregate (e.g., school, district, state) data sets or reports may contain potentially confidential student information. Even nonconfidential student information may be confidential when combined with other data elements and, therefore, will be suppressed as appropriate. Refer to Resource C—Tiers for Release of Data.

F. Breach of Security

In the event of a breach of security, the requirements and procedures related to notification outlined in 2-6-1503, MCA of the Montana Code Annotated will be followed as appropriate.

V. CLOSING

Questions concerning this policy should be directed to the division administrator of the Measurement and Accountability Division.

VI. REFERENCES

- Notification of Breach of Security of Data System—2-6-1503, MCA
- *Family Educational Rights and Privacy Act (FERPA) 34 CFR, Part 99* located at http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

- Montana Secretary of State, Local Government Retention and Disposition Schedule located at http://sos.mt.gov/records/Local/index.asp
- ePass Montana Instructions—https://app.mt.gov/epass/portal/instruct.html

Other useful resources:

- Destruction of Local Government Records—MCA 2-6-1012, MCA 2-6-1201, MCA 2-6-1205
- Transparency and public availability of public school performance data - reporting - availability for timely use to improve instruction—20-7-104, MCA
- Authority of Department to Issue Identification, Cards – Lawful Presence Verification—61-12-501, MCA
- Protection of Personal Information–Compliance—Extensions 2-6-1502, MCA
- Basic system of free quality public elementary and secondary schools defined - identifying educationally relevant factors—establishment of funding formula and budgetary structure - legislative review - 20-9-309, MCA
- POL—Internet Privacy and Security https://montana.policytech.com/docview/?docid=568&public=true
- Montana School Accreditation Standards and Procedures Manual – http://opi.mt.gov/PDf/Accred/Ch55/AccreditationStandards_Ch55.pdf
- OPI Records Management Policy—Chapter 1\1.1.05 Records Management.docx

VII. ATTACHMENTS

VIII. RESOURCES

Resource A—OPI Employee AIM Access Request

Resource B—OPI Employee Confidentiality Agreement

Resource C—OPI Data Tiers for Release of Data

Resource D—OPI Cell Suppression Flow Chart

Resource E—OPI Affidavit of Non-Release

Resource F—Contractor's Employee or Contractor Nondisclosure Statement

Resource G—Researcher-FERPA Memorandum of Understanding

Resource H—FERPA Memorandum of Understanding Audit-Evaluation Exception