

Academic Year 2024-25 Data Use Agreement

MI Student Aid Michigan Department of Lifelong Education, Advancement, and Potential (MiLEAP)

Section 1: High School Information

High School Name		High School SAT Code	
Street Address	City	State MI	Zip Code
High School Web Site		Phone Number	

Section 2: Data Use Agreement Details

Read and understand the details of the Data Use Agreement.

This Data Use Agreement (hereinafter called the {"**Agreement**"}) is entered into by and between the **high school named in Section 1** (hereinafter called {"**Data Receiver**"}), and the Michigan Department of Lifelong Education, Advancement, and Potential (MiLEAP) (hereinafter called "MiLEAP"). Furthermore, Data Receiver, will, for the purposes of this Agreement serve as an authorized representative of MiLEAP. MiLEAP will sometimes be referred to herein as a Data Provider. This Agreement will become effective upon being signed by both parties and will remain effective September 1, 2024 through August 31, 2025.

Definitions

For the purposes of this Data Use Agreement,

- "Personally Identifiable Information (PII)" shall refer to any data elements that could potentially identify a student, parent, or employee, and includes name, address, a personal identifier, such as Social Security number, date of birth, place of birth, etc. as defined in the Family Educational Rights and Privacy Act (FERPA).
- "Confidential information" or "confidential data" shall refer to any non-public information regarding an individual student.

FERPA Regulations and Audit or Evaluation Exception

All data sharing measures will be performed in accordance with the requirements of the Federal "Family Education Rights and Privacy Act of 1974 as amended, (20 U.S.C. §1232g) (FERPA)." FERPA §1232g(b)(1)(C) provides that education records and personally identifiable information (PII) may be released without student or parental consent to "authorized representatives of the Comptroller General of the United States, the Secretary, or State educational authorities" for use in "connection with the audit and evaluation of Federally-supported education programs, or in connection with the enforcement of the Federal legal requirements which relate to such programs: Provided, that except when collection of PII is specifically authorized by Federal law, any data collected by such officials shall be protected in a manner which will not permit the personal identification of students and their parents by other than those officials, and such personally identifiable data shall be destroyed when no longer needed for such audit, evaluation, and enforcement of Federal legal requirements" (FERPA §1232g(b)(3)). Additionally, FERPA regulation 34 CFR §99.31(a)(3) allows disclosure of PII without consent to authorized representatives of a State education authority.

Data Provider Obligations

MiLEAP maintains ownership of the data. The Data Receiver does not obtain any right, title, or interest in any of the data furnished by the provider. MiLEAP ensures all transmissions to the Data Receiver will be via a secured method.

Data Receiver Obligations/Other

The receiver of data maintains a stewardship responsibility for the confidentiality, preservation, and quality of the data. A data steward is responsible for the operational, technical, and informational management of the data.

- Uses and disclosures as provided in this Agreement.* Data Receiver may use and disclose the confidential information provided by the Data Provider only for the purposes of collecting aggregate data on the number of students (and/or percent of students) who completed a Free Application for Federal Student Aid (FAFSA) and only in a manner that does not violate State or Federal privacy regulations adopted by the Data Provider. Only the individuals or classes of individuals will have access to the data that need access to the confidential information to prepare aggregate reports.
- Nondisclosure Except as Provided in this Agreement* Data Receiver shall not use or further disclose the confidential data except as stated in the approved reports. The Data Receiver will not re-disclose data to a third party. "**Third party**" does not include the partners listed on the **Secondary Partner Roster in Section 5.**

- c. *Safeguards.* Data Receiver agrees to take appropriate administrative, technical, and physical safeguards to protect the data from any unauthorized use, access, or disclosure not provided for in this agreement. The Data Receiver agrees to abide by all State and Federal regulations, including FERPA. Data Provider must ensure that PII will be transmitted through secure methods only. Data must be encrypted during all transmissions.
- d. *Reasonable Methods.* Data Receiver agrees to use “reasonable methods” to ensure to the greatest extent practicable that Data Receiver and all parties accessing data are FERPA-compliant. Specifically, this means:
 - 1. PII may only be used to carry out an audit or evaluation of State or Federal supported education programs, or for the enforcement of or compliance with, Federal legal requirements related to these programs.
 - 2. Data Receiver must protect PII from further disclosures or other uses, except as authorized by Data Provider in accordance with FERPA. Approval to use PII for one audit or evaluation does not confer approval to use it for another.
- e. *Confidentiality.* Data Receiver agrees to protect data and information according to acceptable standards and no less rigorously than they protect their own confidential information. Identifiable level data will not be reported or made public.
- f. *Reporting.* Data Receiver shall report to the Director of MI Student Aid immediately, once the Data Receiver becomes aware of any use or disclosure of the confidential information in violation of this agreement or applicable law.
- g. *Public Release.* No confidential information will be publicly released.
- h. *Data Retention/Destruction of Records at End of Activity.* Records must be destroyed in a secure manner at the end of the work described in the work proposal. Data Receiver agrees to send a written notice that the data has been properly destroyed within 30 days of the end of the work as described in the proposal. However, any de-identified data may be retained for future use. As a courtesy, Data Provider requests to be informed of future uses of de-identified data.
- i. *Proper Disposal Methods.* In general, proper disposal methods may include, but are not limited to:
 - 1. For PII in paper records, shredding, burning, pulping, or pulverizing the records so that PII is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
 - 2. For PII on electronic media, clearing (using software or hardware products to overwrite media with non-sensitive data), purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains), or destroying the media (disintegration, pulverization, melting, incinerating, or shredding).
 - 3. Other methods of disposal also may be appropriate, depending on the circumstances. Organizations are encouraged to consider the steps that other data professionals are taking to protect student privacy in connection with record disposal.
- j. *Minimum Necessary.* Data Receiver attests that the confidential information requested represents the minimum necessary information for the work as described in the Agreement and that only relevant individuals will have access to the confidential information in order to perform the work.
- k. *Authorizations.* The Data Receiver agrees to obtain individual authorizations from those who will be granted access to use the confidential information. Documentation of these authorizations must be provided to Data Provider prior to receipt of the confidential information.
- l. *Data Ownership.* Data Provider is the data owner. Data Receiver does not obtain any right, title, or interest in any of the data furnished by Data Provider.
- m. *Publication/release requirements.* If applicable, Data Receiver will notify Data Provider when a publication or presentation is available and provide a copy upon request.
- n. *Data Breach.* Per the Identity Theft Protection Act 452 of 2004, 445.72, in the event of a data breach the Data Receiver will be responsible for contacting and informing any parties, including students, which may have been affected by the incident or security breach. The Data Receiver is responsible for any costs incurred by the Data Receiver in responding to the breach. It should be noted that by signing this Agreement, the signatory accepts responsibility for data security. MiLEAP has the right to terminate the Agreement when a breach has occurred and the Data Receiver cannot demonstrate proper safeguards were in place to avert a breach. MiLEAP must approve the resolution to the breach.
- o. *Non-Financial Understanding.* This Agreement is a non-financial understanding between Data Provider and Data Receiver. No financial obligation by or on behalf of either of the parties is implied by a party’s signature at the end of this agreement.
- p. *Liability.* Each Party to this Agreement shall be liable for the actions and omissions of its respective employees and partners.

If, as a result of the high school’s failure to perform as agreed, the Data Receiver is challenged by a governmental authority or third party as to its conformity to or compliance with State, Federal, and local statutes, regulations, ordinances, or instructions; the Data Receiver will be liable for the cost associated with loss of conformity or compliance.

Purpose

Data sharing under the audit or evaluation exception may only be done to the extent necessary to carry out an audit or evaluation of State or Federal supported education programs, or to enforce or comply with Federal legal requirements that relate to those programs.

Scope of Work

The Parties desire to cooperate with each other in sharing information contained in student education records for the purposes of study and research to assist the high school in identifying Tuition Incentive Program (TIP) eligible students or students who have or will complete a FAFSA as defined by the U.S. Department of Education.

All data exchanges will be conducted via secure methods.

Section 3: Data Receiver Designee Employee Access Roster**(Employees of the high school or ISD/RESA/ESA)**

List only employees at the high school or Intermediate School District (ISD)/Regional Educational Service Agency (RESA)/Educational Service Agency (ESA). Those individuals listed will access data about the students at your high school, including FAFSA completion, TIP eligibility rosters, student look-ups, and qualifier lists. All names listed are subject to verification and approval from MI Student Aid. MI Student Aid reserves the right to revoke or suspend access to MiSSG at any time.

NOTE: At any time, email mistudentaid@michigan.gov to remove individual(s) who should no longer have access to MiSSG.

First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address
First Name	Last Name	Email Address

Section 4: College Advising Corps Designee (Only Employees of AdviseMI, MCAC, or MSUCAC)

The designee(s) listed are college adviser(s) who are employed with one of the three college advising corps (AdviseMI, Michigan College Advising Corp [MCAC], Michigan State University College Advising Corp [MSUCAC]). The designee(s) listed will access data about the students at your high school, including FAFSA completion, TIP eligibility rosters, student look-ups, and qualifier lists.

The designee(s) must complete the MiSSG training and complete/return the Acknowledgement of Use before a MiSSG user account is created. All names listed will be verified by MI Student Aid. MI Student Aid reserves the right to revoke or suspend access to MiSSG at any time.

NOTE: At any time, email mistudentaid@michigan.gov to remove individual(s) who should no longer have access to MiSSG.

First Name and Last Name	Email Address	College Advising Corp
First Name and Last Name	Email Address	College Advising Corp

Section 5: Secondary Partner Roster (Community organization/foundation, local college access networks, etc.)

*This section is optional. Please list the community organization/foundation or local college access network group partner(s) who have your approval to review your students' data, **if any**. The partner(s) **will not have a user account or direct access to MiSSG**. The individuals listed below shall only receive and review information that the data designees listed in Section 3 choose to share from MiSSG. **Liability for misuse of data remains with the principal/superintendent listed in Section 7.***

First Name and Last Name	Affiliated Organization	Email Address	Phone Number
First Name and Last Name	Affiliated Organization	Email Address	Phone Number
First Name and Last Name	Affiliated Organization	Email Address	Phone Number
First Name and Last Name	Affiliated Organization	Email Address	Phone Number

Section 6: How to Submit the Form

- 1. Complete the form.** (Please type as handwritten forms will cause processing delays.)
- 2. Principal/superintendent must email this form as an attachment to mistudentaid@michigan.gov.**

NOTE: Please note that once we have received the DUA, it has not been fully processed (or considered "DUA on file") until the user(s) listed on the DUA received their welcome email. The welcome email will contain their user name, temporary password, and login instructions.

Section 7: Principal/Superintendent Signature

The high school's principal/superintendent must complete the document by signing this agreement.

Principal or Superintendent Name		Principal or Superintendent Title	
Principal or Superintendent Email Address		Principal or Superintendent Phone Number	
/s/	Principal or Superintendent Signature		Date of Signature

My signature certifies that:

- I am the principal or superintendent of the high school identified in Section 1.*
- I have read and understand the Data Use Agreement Details in Section 2.*
- Any Data Receiver Designee listed in Section 3 is an **employee at my high school or ISD/RESA/ESA**.*
- Any College Advising Corp employee listed in Section 4 is a **college adviser in one of the three college advising corps (AdviseMI, MSUCAC, MCAC)**.*
- Any Secondary Partners listed in Section 5 is a partner who has my approval to review my students' data.*
- I will email mistudentaid@michigan.gov to **remove individual(s)** who should no longer have access to MiSSG.*

Section 8: Data Provider Points of Contact Information

Diann Cosme, Director, MI Student Aid

Michigan Department of Lifelong Education, Advancement, and Potential

P.O. Box 30462
Lansing, MI 48909

888-447-2687

mistudentaid@michigan.gov

Section 9: Data Provider Signature – MiLEAP Use Only



Diann Cosme, Director
Michigan Department of Lifelong Education, Advancement, and Potential