

Academic Year 2016-17 Data Use Agreement

1. High School Information

Enter high school name, SAT code, and address information. Read the following agreement and then complete and sign page 3. This agreement must be submitted to Student Scholarships and Grants (SSG) with a completed Data Receiver Designee Form (Form 5360).

**Michigan Department of Treasury
Student Financial Services Bureau
Student Scholarships and Grants**

High School Name		High School SAT Code	
High School Street Address	City	State	ZIP Code

2. Data Use Agreement Details

This Data Use Agreement (hereinafter called the {"**Agreement**"}) is entered into by and between the **above named high school** (hereinafter called {"**Data Receiver**"}), and the Michigan Department of Treasury (hereinafter called "Treasury"). Furthermore, Data Receiver, will, for the purposes of this Agreement serve as an authorized representative of Treasury. Treasury 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, 2016 through June 30, 2017.

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"/"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

The Michigan Department of Treasury 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. Treasury 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.

- a. *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) that 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.

- b. *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 attached Secondary Security Access form.**
- 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 be not reported or made public.
- f. *Reporting.* Data Receiver shall report to Carla Foltyn, Student Scholarships and Grants (SSG) 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 on behalf of Data Receiver, the signatory accepts responsibility for data security. Treasury 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. Treasury 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.

3. High School Principal Signature

Data Receiver Point of Contact/Data Custodian will complete, sign, and submit along with a completed Form 5360.

High School Administrator Name	Title
Administrator E-mail Address	High School Telephone Number

/s/	Administrator Signature	Date of Signature
-----	-------------------------	-------------------

The attached Data Receiver Designee form is to list a counselor(s) in your high school or Intermediate School District (ISD) who will have access to MiSSG for the purpose of viewing student Free Application for Federal Student Aid and Tuition Incentive Program (FAFSA/TIP) data. The designee(s) must be an employee of your high school or ISD and housed within your high school building.

The attached Secondary Security Access form is to list a partner(s) who has your approval to review the report with your students.

4. Data Provider Point of Contact

Carla Foltyn
Director, Student Scholarships and Grants Division
Michigan Department of Treasury/Student Financial Services Bureau
1-888-447-2687
PO Box 30462
Lansing, Michigan 48909

Anne Wohlfert
Director, Student Financial Services Bureau
Michigan Department of Treasury/Student Financial Services Bureau
1-888-447-2687
PO Box 30462
Lansing, Michigan 48909

5. Treasury Use Only

Data Provider Designated Signatory		Date
------------------------------------	---	------