



EXECUTIVE SUMMARY

Student Data Privacy, Disclosure and Security Policy

Last Updated 8/5/2022

The Center for Educational Performance and Information is chiefly responsible for coordinating the collection, management and reporting of all Michigan education data required by state and federal law. CEPI and the Michigan Department of Education are committed to protecting confidential education records, and to transparency when it comes to data collection, storage and disclosure.

Our protocols follow strict State of Michigan standards and best practices. Our privacy policies and procedures meet or exceed the data sharing guidelines of the [Family Educational Rights and Privacy Act](#).

CEPI's full [Data Systems Privacy and Security Policy](#) is available on our website. See also [How CEPI Protects Education Data](#).

General

- Education data are safeguarded and privacy is honored, respected and protected.
- Protecting students' privacy and data security is taken seriously. That same level of diligence is required of all stakeholders and users.
- CEPI and MDE ensure that those with education data access understand their ethical and legal obligation to keep records confidential.
- Data retention and disposal schedules are followed.
- Data governance structures are used to establish and maintain checks and balances of safeguards.
- CEPI and MDE adhere to Michigan Department of Technology, Management and Budget policies and procedures to protect records from loss, theft, vandalism, illegal access and corruption.
- The designated Chief Data Privacy Officer oversees privacy and security policies and practices as they pertain to CEPI and MDE data.
- Concerns about security breaches are immediately reported to the respective office director and Chief Data Privacy Officer in accordance with CEPI/MDE procedures.
- Data access provisions may change if mandated by state or federal law. Thus, these policies may change to be consistent with state and federal law.

Data Collection

- CEPI facilitates and streamlines data collections using secure web-based applications.
- Secure, role-based levels of data access are enforced and monitored.
- Access to a secure application is only granted based on FERPA-compliant justification.

- Access is removed once a user no longer performs the relevant, critical functions. CEPI also performs an annual audit of PII access rights.
- Automatic encryption and Secure Socket Layer techniques are used for data transmission.
- CEPI assigns a unique/personnel identifier code for all students and educators. This enables names and dates of birth, for example, to be removed from the stored data to safeguard privacy.

Data Storage

- CEPI maintains the Michigan Statewide Longitudinal Data System to store and connect data.
- Data are hosted on a secure platform that provides the highest level of security along with backup and disaster recovery capability.
- Access to MSLDS is only granted based on FERPA-compliant justification. Access requests are reviewed by both CEPI and MDE.
- Access is removed once a user no longer performs the relevant, critical functions. CEPI also performs an annual audit of MSLDS access rights.

Data Disclosure

- The release of personally identifiable information (PII)¹ is governed by the Family Educational Rights and Privacy Act (FERPA) and other applicable state and federal privacy laws.
- Access to confidential data is always purposeful, regulated and governed by laws. Access is only provided to authorized individuals with a legitimate educational need who work to improve teaching and learning in Michigan.
- Aggregate data are disclosed by default. If individual-level data must be disclosed, it is deidentified (made anonymous by removing unique identifiers and other information that could reveal the identity of a student). PII is only disclosed when necessary.
- Only the minimal data required for an audit or program evaluation are shared.
- Individual student record data are not disclosed under Freedom of Information Act requests.
- Data that identify the names of individual students are not released to the public.
- Sharing or selling any student-level data with any person or organization seeking to promote their products or services does not occur.
- All reports CEPI and MDE develop are for purposes that support state policy-making as well as state and federal compliance reporting.

¹ PII for education records is a FERPA term referring to identifiable information that is maintained in education records and includes direct identifiers (such as a student's name, address or identification number/code), indirect identifiers, (such as gender, race, date of birth, place of birth or geographic indicator) or other information that can be used to distinguish or trace an individual's identity, directly or indirectly, through linkages with other information.

- CEPI and MDE develop reports in aggregate form and make them available to the public with proper data disclosure avoidance techniques (e.g., cell suppression of cells containing less than 10) to help protect data confidentiality.
- CEPI and MDE develop reports in aggregate form and make them available to local, state and federal employees with a legitimate educational need.
- CEPI and MDE develop individual student record-level reports, with and without student identifiers, and make them available to authorized users with a legitimate educational need when this information is needed to improve teaching and learning in Michigan.
- PII (e.g., student's name, address, date of birth, dates of attendance, district of enrollment) may be released as requested by human services or law enforcement representatives in accordance with FERPA, which allows for such release without parental consent when it is necessary to protect the health or safety of the student or other individuals.
- The state does not designate directory information, nor provide opportunities for "opting out" of sharing directory information. Thus, directory information is only shared by the state with authorized school users for purposes of enrollment.
- If an individual requests to inspect and review their own or their child's state education records, the individual is directed to follow the FERPA request process, which requires verification of the requester's identity and rights to the records.
- If an authorized representative who receives data to perform audits, evaluations or compliance activities improperly discloses the data, the representative may be denied further access to student PII for at least five years and subject to review and legal implications imposed by the United States Department of Education, Family Compliance Office.
- **Data Disclosure: Internal (State of Michigan) Staff:**
 - PII is only released to authorized representatives who have received clearance to access the data for a legitimate need to support their professional roles.
 - Employees who have access to student-level data undergo privacy and security training specific to FERPA. Those with roles responsible for data sharing undergo additional privacy and security training.
 - Employees responsible for analyzing the data and developing reports shall access the data and utilize it internally and share results with authorized employees who have demonstrated a legitimate educational need.
 - If the data are to be disclosed to another state agency for an approved purpose, a formal data sharing agreement is established to ensure compliance with all laws and policies governing the data.
- **Data Disclosure: Third Parties**
 - Approved contractors and researchers sign a confidentiality agreement that outlines acceptable data storage, use, disposal and reporting requirements of CEPI and MDE.

- All contractors and researchers must complete training on the ethical and professional standards for protecting human research participants that are either the same as, or equivalent to, the training CEPI and MDE employees complete.
- Data are disclosed to researchers auditing or evaluating education policies or conducting studies for FERPA-allowable reasons after a rigorous proposal application review process by the [Michigan Education Research Institute](#), a partnership between CEPI, MDE and several other groups. By default, direct identifiers are not provided, and the state identification code is replaced with a researcher code.
- Data are disclosed to contractors who are auditing or evaluating Michigan education policies and assisting in the development of state data applications and tools. A formal data sharing agreement or contract is established to ensure compliance with all laws and policies governing the data.
- If PII is disclosed to researchers or contractors, CEPI and MDE enter into a written agreement that:
 - i. designates the individual who will serve as the authorized representative
 - ii. specifies the purpose, scope and duration of the project and the information to be disclosed
 - iii. requires the PII to only be used to meet the purpose of the disclosure
 - iv. prohibits the use of the personal identification of an individual by anyone other than the agreed upon representatives of the organization with legitimate interests
 - v. affirms that the authorized representative can only publish results in a way that protects the privacy and confidentiality of the individuals involved
 - vi. requires the authorized representative to destroy the PII when the information is no longer needed and to document the appropriate technical, physical and administrative safeguards used to protect the PII data at rest and in transit
 - vii. includes a plan for how to respond to a data breach
- Educators who have a legitimate educational interest may be granted access to PII data for their education entity's data. Access is authorized by the school, district or intermediate school district's leadership, who ensure that the user agrees to comply with proper privacy and security protocols.

Questions:

Questions regarding these policies should be directed to CEPI customer support at cepi@michigan.gov.