CENTER FOR EDUCATIONAL PERFORMANCE AND INFORMATION

MICHIGAN Department of Education

EXECUTIVE SUMMARY
STUDENT DATA PRIVACY, DISCLOSURE AND SECURITY POLICY

Policies used by the Center for Educational Performance and Information (CEPI) and the Michigan Department of Education (MDE) to safeguard and release student educational record data.

General

1. Education data are safeguarded and privacy is honored, respected and protected.
2. Protecting students' privacy and data security is taken seriously, and that same level of diligence is required of all stakeholders and users.
3. CEPI and MDE will ensure that those with education data access understand their ethical and legal obligation to keep records confidential.
4. Role-based secured levels of data access are enforced and monitored.
5. Data retention and disposal schedules are followed.
6. Data governance structures are utilized to establish and maintain checks and balances of safeguards that are implemented.
7. CEPI and MDE will adhere to Department of Technology, Management and Budget (DTMB) policies and procedures put in place to protect records from loss, theft, vandalism, illegal access and corruption.
8. Data are hosted on a secure platform that provides the highest level of security along with backup and disaster recovery capability.
9. Automatic encryption and Secure Socket Layer (SSL) techniques for data transmissions are used.
10. The designated Chief Data Privacy Officer will oversee the privacy and security policies and practices as they pertain to CEPI and MDE data respectively.
11. Concerns about security breaches are reported immediately to the respective office director and Chief Data Privacy Officer in accordance with CEPI/MDE procedures.
12. Data access provisions may change if mandated by state law or federal law. Thus, these data policies may change to be consistent with state and federal law.

Data Disclosure

1. Release of personally identifiable information (PII)* is always governed by the Family Educational Rights and Privacy Act (FERPA) and other applicable state and federal privacy laws.
2. Access to confidential data is always purposeful, governed by laws, regulated and provided to authorized individuals with a legitimate educational need who work to improve teaching and learning in Michigan.
3. Aggregate data are disclosed by default. If individual-level data must be disclosed, it will be de-identified (i.e., records made anonymous by removing unique identifiers and other information that could trace the identity of the student). PII is only disclosed when necessary.
4. Only the minimal data that are required for an audit or program evaluation are shared.
5. Individual student record data are not disclosed under Freedom of Information Act (FOIA) requests.
6. Data that identifies the names of individual students is not released to the public.
7. Sharing or selling any student-level data with any person or organization seeking to promote their products or services does not occur.

8. 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) applied to help protect data confidentiality.
9. CEPI and MDE develop reports in aggregate form and make them available to local, state and federal employees with a legitimate educational need.
10. 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.
11. All reports CEPI and MDE develop are for purposes that support state policy-making as well as state and federal compliance reporting.
12. PII (i.e., 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.
13. 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.
14. If an individual requests to inspect and review their own or 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.
15. 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.

A. Internal Staff

1. PII will only be released to authorized representatives who have received clearance to access the data for a legitimate need to support their professional roles.
2. 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.
3. 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.
4. 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.

B. Third Parties

1. Approved contractors and researchers sign a confidentiality agreement which outlines acceptable data storage, use, disposal and reporting requirements of CEPI and MDE.
2. 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 state of Michigan's MDE-CEPI Internal Review Board (IRB). In addition, all researchers must have completed training on the ethical and professional standards for protecting human research participants that are either the same as, or equivalent to, the training that

CEPI and MDE employees complete. By default direct identifiers are not provided, and the state identification code is replaced with a researcher code.

3. 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. In addition, all contractors must have completed training on the ethical and professional standards for protecting these data that are either the same as, or equivalent to, the training that CEPI and MDE employees complete.
4. If PII is disclosed to researchers or contractors, CEPI and MDE enter into a written agreement that:
    - designates the individual that will serve as the authorized representative
    - specifies the purpose, scope and duration of the project and the information to be disclosed
    - requires the PII to only be used to meet the purpose of the disclosure
    - does not permit the personal identification of an individual by anyone other than the agreed upon representatives of the organization with legitimate interests
    - affirms that the authorized representative can only publish results in a way that protect the privacy and confidentiality of the individuals involved
    - 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
    - includes a plan for how to respond to a data breach
5. 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 ensures that the user agrees to comply with proper privacy and security protocols.

* 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 which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.