Rules of
Department of Elementary and Secondary Education
Division 20—Division of Learning Services
Chapter 700—Office of Data System Management

Title 5—DEPARTMENT OF ELEMENTARY AND SECONDARY EDUCATION

Division 20—Division of Learning Services

Chapter 700—Office of Data System Management

5 CSR 20-700.100 Statewide Longitudinal Data System

PURPOSE: This rule explains the data collected by the Department of Elementary and Secondary Education within the statewide longitudinal data system commonly known as the Missouri Comprehensive Data System (MCDS). The rule also addresses the procedures that are used to ensure the confidentiality of student records maintained in the MCDS.

(1) Data Inventory.

(A) The Department of Elementary of Secondary Education (department) publishes annually an inventory of student data collected and posted on the department's website.

(B) The department shall notify annually to the governor, president pro tempore of the senate, the speaker of the house, and the joint committee on education any changes to existing data elements.

(2) Data Access and Management Policies.

(A) The department adheres to the confidentiality requirements of both federal and state laws including, but not limited to, the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), the Protection of Pupil Rights Amendment (PPRA), and the National School Lunch Act. These policies include:

1. Defining privacy, confidentiality, personally identifiable information, disclosure, access, and confidential data; and
2. Maintaining adequate privacy and confidentiality protections; including the assignment of a unique student identifier, data security, restricted access, and reasonable statistical disclosure.

(3) Data Requests.

(A) Requests must be submitted to the department in writing including, but not limited to, what data are being requested, the purpose of the request, for whom the study is being conducted, and how the requestor will ensure data confidentiality and security. Requests including student level data will require a Memorandum of Agreement (MOA) and research IDs will be created for all records.

(B) All recipients/users of the requested information must sign a MOA that includes:

1. Introduction and Relationship;
2. Data Being Requested;
3. Scope of Activities;
4. Participant Non-disclosure;
5. Confidentiality/Redisclosure;
6. Transfer/Storage/Disposal;
7. Release of Analyses;
8. Right to Audit; and
9. Agreement Period, Amendment, and Termination.

(4) Data Security Plan. The department, in cooperation with the Office of Administration Information Technology Service Division (OA-ITSD), reviews and maintains the data security plan. This includes, but is not limited to:

(A) Guidelines for authentication of authorized access;

(B) Privacy compliance standards;

(C) Privacy security audits;

(D) Breach planning, notification, and procedures;

(E) Data retention and disposition policies; and

(F) Data security policies including electronic, physical, and administrative safeguards.

AUTHORITY: sections 161.092 and 161.096, RSMo Supp. 2014. Original rule filed Jan. 22, 2015, effective Aug. 30, 2015.*

**Original authority: 161.092, RSMo 1963, amended 1973, 2002, 2003, 2013 and 161.096, RSMo 2014.*