

Statewide Educational Data Warehouse Project Policy Statement

Legal Authorities

The Data Warehouse is created and shall be used in accordance with state and federal legal authorities that govern information exchange and access, and confidentiality of student records and personally identifiable information. Storing state data (e.g., data from the Department's Student Information Management System (SIMS), the Massachusetts Comprehensive Assessment System (MCAS) database, and the Education Personnel Information Management System (EPIMS)) and local data (e.g., data that a school district chooses to load into the Data Warehouse) in the Data Warehouse does not create new rights of access for the Department of Education or for participating school districts to the data loaded in the Data Warehouse. Rather, the Data Warehouse is a new tool for storing and reporting data that is intended to increase the ability of school districts and the Department to use data to improve education policy and practice in the Commonwealth.

Each school district participating in the Data Warehouse project is authorized by state and federal laws to release to the Department of Education aggregate data and personally identifiable data about students enrolled in the district and staff employed by the district for the purpose of improving public education in the Commonwealth. The authority to release student record information to the Data Warehouse derives, in part, from the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99. FERPA authorizes schools and districts to disclose education records to the Department of Education without parental consent in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement or compliance with federal legal requirements relating to those programs. 34 CFR § 99.35.

Consistent with federal law, a participating school district may have access to its own local data stored in the Data Warehouse, to individually identifiable data about its students that the district has submitted to the databases maintained by the Department, and to non-personally identifiable aggregate data from all schools and districts in the Commonwealth that are stored in the Data Warehouse. A participating school district may not release personally identifiable student data to another district without parental consent or unless the student about whom the records pertain seeks or intends to enroll in the second district. 34 CFR § 99.31(a)(2); M.G.L. c. 71, § 37L. The Department of Education may not allow one district to have access to confidential data from another district from the Data Warehouse except as permitted by law.

The Commissioner of Education is authorized by state law to review records maintained by schools and districts when those records are necessary for supervising public schools and evaluating state and federal programs. M.G.L. c. 69, §§ 1A and 1I. The local data that participating schools and districts may store in the Data Warehouse are currently available by law to the Commissioner in any and all forms in which the data are maintained, whether at the local level or in the Data Warehouse.

In fulfillment of the Commissioner's statutory authorities and obligations, the Department of Education will access local data stored in the Data Warehouse consistent with applicable state and federal laws. The Department of Education will continue current practices of working cooperatively with public schools and districts to review local data and information and will provide notice to the interested school or district prior to accessing local data as described below.

User Agreements

Recognizing the importance of maintaining confidentiality and ensuring proper use of the data in the Data Warehouse, the Department and school districts participating in the Data Warehouse project are committed to abiding by the confidentiality provisions outlined below and as required by state and federal laws, and with the rights and responsibilities of access described below. Also, the Department and participating schools and districts recognize that state and federal laws prohibit unauthorized disclosure of any confidential information, and improper disclosure of confidential information may result in penalties including but not limited to restrictions on access to the Data Warehouse.

As with any confidential information in the custody of the Department of Education, the Department will authorize certain personnel to have access to the Data Warehouse in accordance with current Department policy and practice, and state and federal laws, only if those personnel have a legitimate need to access that information to fulfill their job duties as agents of the Commissioner and the Department. Authorizations for access by Department of Education personnel shall include approval by Department administrators as well as signed confidentiality agreements from each authorized employee. Also, authorized users of the Data Warehouse will be required to participate in user training. The Department will maintain a list of agency authorized users and reasons for access to the Data Warehouse.

When the Department intends to access local data stored in the Data Warehouse, the Department will notify the superintendent and/or the district's Data Warehouse liaison of the subject district. Notice shall include the purpose for accessing local data and a description of the local data that the Department will review. Recognizing that the lack of uniform reporting standards for local data affects the validity and reliability of the local data stored in the system, the superintendent or his/her designee will be given the opportunity to provide the Department with additional information that will assist the Department in fairly and accurately interpreting the local data, as well as an opportunity to discuss the data and related information with the Department.

Participating schools and districts shall designate local staff members who are authorized school or district users permitted to upload information to the Data Warehouse and/or access confidential information from the Warehouse, in accordance with the district's responsibilities under state and federal laws. School and district officials will ensure that authorized local personnel have legitimate educational interests in accessing confidential information and that access is required to perform their duties. See 34 CFR § 99.31(a)(1); 603 CMR 23.02 ("authorized school personnel") and 603 CMR 23.07(3). Also, authorized local personnel must participate in training about the Data Warehouse and comply with locally designed confidentiality policies and practices. School and district confidentiality policies shall be

adopted and updated as needed, in accordance with state and federal laws and this policy statement, to address unique issues related to the Data Warehouse and access to it.

Confidentiality Policies

To ensure that confidential data, including data on individual students, is not created, collected, stored, maintained, or disseminated from the Data Warehouse in violation of state and federal laws and is not used for unauthorized purposes, school districts participating in the Data Warehouse shall adopt policies governing access and confidentiality of data maintained in the Data Warehouse. Only district personnel with a legitimate educational interest may have access to personally identifiable information in the Data Warehouse. Districts should consult with their legal counsel to create policies for data access and confidentiality that include the following information:

- an overview of state and federal confidentiality laws, including the state student records regulations (603 CMR 23.00); the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 CFR Part 99; and the public records law, M.G.L. c. 66, § 10 and M.G.L. c. 4, § 7 Cl. Twenty-sixth;
- a description of limitations on access to and disclosure of confidential information consistent with applicable state and federal laws, including only to those district employees who have a legitimate educational interest;
- the process for approving requests for access to the Data Warehouse, including levels of access if appropriate;
- reporting policies, including requirements for generating reports using the Data Warehouse, restrictions on publication of names or other personally identifiable information and subgroup suppression, and approval processes;
- the physical and electronic security of computer systems (e.g., services, desktops and laptops), including password protection, encryption, restrictions on storage of data on unsecured computer systems or on personal systems;
- the restriction on transmission of data through insecure means such as email;
- the consequences for improper disclosure of and access to confidential information consistent with state and federal laws;
- the data destruction schedules consistent with the student records regulations and applicable records retention schedules; and
- signed confidentiality agreements from all district users.

The Department shall implement similar policies and protocols governing access to the Data Warehouse by its employees.

Third Party Access to Information in the Data Warehouse

As defined in the public records law, all data stored in the Data Warehouse is “made or received” by a public authority and therefore is presumed to be a public record unless otherwise exempted by law as defined in M.G.L. c. 4, § 7 Cl. Twenty-sixth. The Department of Education, as custodian of the Data Warehouse, is required to respond to third party requests (i.e., requests from someone who is not an authorized user of the Data Warehouse) for data from the Data

Warehouse consistent with all applicable laws. The Department must consider its obligations under FERPA; the Massachusetts public records law; and the Fair Information Practices Act (FIPA), M.G.L. c. 66A, in responding to requests for data. Similarly, school districts must respond to third party requests for information from the Data Warehouse consistent with their obligations under FERPA; the Massachusetts Student Records Regulations, 603 CMR 23.00; and the public records law. The public records law does not require a public agency to create a document or record that does not already exist; it requires that the agency provide, upon request, a copy of any public record that the agency maintains that is responsive to a request for records or information.

Student records are confidential records as defined in state and federal law, and are not public records.¹ Disclosure of personally identifiable student record information without consent of the student or the student's parent is permitted only under exceptional circumstances, including to federal, state and local education officials with legitimate educational interests as described above. Unlike student records, certain data about public employees are not strictly protected by law and therefore are generally considered "public records" that are subject to disclosure upon request. However, some information about a public employee is considered to be confidential and is not subject to disclosure. Those exemptions from disclosure are governed by the definitions included in the public records law at M.G.L. c. 4, § 7 Cl. Twenty-sixth.

Examples of public employee records that are exempt from disclosure and may not be released without consent of the employee are:

1. personnel files or information²(e.g., employment applications, performance evaluations, disciplinary documentation, and promotion, demotion or termination information, and information that is "useful in making employment decisions regarding the employee)³;
2. materials or data relating to a specifically named individual, the disclosure of which may constitute an unwarranted invasion of personal privacy⁴ (e.g., Social Security number, marital information, personal financial information);
3. medical files or information⁵;
4. home addresses and home phone numbers of public employees⁶;
5. Criminal Offender Record Information (CORI)⁷;
6. scores on the Massachusetts Tests for Educator Licensure (MTEL) and dates of tests taken⁸; and
7. grades on transcripts and grade point average⁹.

¹ Records are not public records if they are specifically exempted from disclosure by statute. M.G.L. c. 4, § 7 Cl. 26(a). Personally identifiable student records are expressly exempted from disclosure under FERPA and the Student Records Regulations.

² M.G.L. c. 4, § 7 Cl. 26(c).

³ *Wakefield Teachers Assn. v. School Committee*, 431 Mass. 792, 798 (2000).

⁴ M.G.L. c. 4, § 7 Cl. 26(c). Application of this clause of exemption (c) requires a balancing test to determine whether the individual's privacy interest in nondisclosure outweighs the public interest in disclosure.

⁵ M.G.L. c. 4, § 7 Cl. 26(c).

⁶ M.G.L. c. 4, § 7 Cl. 26(o).

⁷ M.G.L. c. 6, § 172.

⁸ M.G.L. c. 4, § 7 Cl. 26(c).

⁹ M.G.L. c. 4, § 7 Cl. 26(c).

In contrast, certain information about school staff is a public record that is subject to disclosure upon request.¹⁰ Staff information that a public school or school district, or the Department of Education, is required to release to a third party upon request includes but is not limited to:

1. staff names;
2. salary information;
3. staff positions and teaching assignments, including class schedules;
4. certification or licensure status and areas of certification;
5. educational institutions attended and degrees earned, including areas of study; and
6. Highly Qualified (HQ) status, including how the teacher has achieved HQ status.

If the Department of Education receives a third party request for local data (i.e., a request from a non-authorized user), the Department of Education will refer the requester to the school district(s) whose data is sought. The Department is, however, required to respond to requests for records in its custody consistent with its legal obligations under the public records law.

Therefore, if a requester insists that the Department provide it with local data stored in the Data Warehouse, the Department will notify the district of the request and of its proposed response, and will share with the subject school or district a copy of its response that includes only records that are not exempt from disclosure. The Department will respond to requests for information from the state-maintained databases included in the Data Warehouse consistent with its obligations under the public records law.

More information about the public records law, including agencies' obligations under the law and exemptions, is available in *A Guide to the Public Records Law* published by the Supervisor of Public Records and available at <http://www.sec.state.ma.us/pre/preidx.htm>. Districts may wish to consult with their legal counsel about their obligations under these laws, and as they adopt confidentiality policies and protocols.

Dated: July 18, 2007

¹⁰ This is consistent with the requirements under the federal No Child Left Behind Law (NCLB) that districts must notify parents of their right to request information related to the professional qualifications of their children's classroom teachers.