

Chapter 2 Security and Training Table of Contents

Security and User Administration	1
Maintaining Confidentiality	1
Suppressing Aggregate Data for Small Groups.....	2
Directory Administrator Responsibility	2
Figure 1 – User Credentials and EDW Data Access	3
District Data Access Policy	3
Training District Users	3
EDW Training Curriculum	4

Security and User Administration

Confidential Data

According to federal law, a school or district may disclose personally identifiable information from a student’s education record without consent to “other school officials, including teachers, within the [school or district] whom the [school or district] has determined to have legitimate educational interests.” [FERPA](#) at 34 CFR § 99.31(a)(1). The standard in Massachusetts is, arguably, even more strict. As described in the state Student Records Regulations at [603 CMR 23.00](#) (see the definition of “authorized school personnel” in 23.02), no individuals or entities other than the parent, eligible student, or *school personnel working directly with the student* are allowed to have access to information in the student record without the specific, informed, written consent of the parent or eligible student.

The Education Data Warehouse (EDW) contains both public and confidential information. Examples of public information include:

- Aggregated school, district, and statewide test results that *do not contain* a list of student characteristics that would make it possible to identify a student’s test results
- Staff name, position

Examples of confidential information include:

- Aggregated school, district, and statewide test results that contain a list of student characteristics that would make it possible to identify a student’s test results
- Student home address and test results
- Staff home address

When a district or school user runs one of the state’s predefined reports, only the authorized information for that user’s district or school is returned, depending on the user’s security role and district or school affiliation in Directory Administration. This conditional access to confidential also extends to the aggregate data displayed in the state’s predefined reports. Report Studio, the Cognos application used to create predefined reports, supports conditional suppression. However, PowerPlay Web analysis cubes do not support conditional suppression so it is important that your district’s EDW planning team as well as district users understand the rules regarding the confidentiality of some aggregate data.

Suppressing Aggregate Data for Small Groups

According to federal education laws, confidential information includes “a list of personal characteristics or other information that would make it possible to identify the child with reasonable certainty.”¹ Consequently, it is Department policy that public reports containing aggregate student performance data must suppress results for small groups of students when associated with characteristics that would make it possible to identify a student. This policy applies to public reports whenever an identified group contains

- fewer than 10 students for MCAS data or
- fewer than 6 students for SIMS data.

When an identified group is smaller than these thresholds, the report must display a placeholder (for example, -, *, NA) with a disclaimer explaining what the placeholder means. The School/District Profile reports (<http://profiles.doe.mass.edu/>) provide examples of appropriate suppression.

Predefined reports created by the Department apply conditional suppression rules but PowerPlay Web analysis cubes do not support conditional suppression. Districts should limit cube access to users within a single district who have a legitimate educational need for the information and work directly with the students identified. Users who are given access to cubes should understand small group suppression rules and be careful not to share reports they create from the analysis cubes with unauthorized users.

District report authors also should be aware of small group suppression rules. They are responsible for ensuring that the Department’s suppression policy is applied appropriately to any reports they create.

Directory Administrator Responsibility

As explained in Chapter 1, *Overview and Login*, access to the EDW is gained and controlled by the assignment of security roles in Directory Administration (DA). Within DA, these roles are based on an individual’s association with a district or school code. If a district’s one or more Directory Administrators are not part of the EDW project team, it is the responsibility of the Data Warehouse Contact and the team to ensure that the security roles for the EDW are assigned correctly and with proper authority.

If an individual is associated with a school code in DA, the only security role you can assign is DW – (211) School User. If an individual is associated with a district code in DA, you can choose to assign *either* the DW – (210) District User role or, if this person will be authoring reports as well as reviewing existing reports, the DW – (209) District Report Author role.

Note: It is important to understand that the three security roles (209, 210, and 211) are mutually exclusive. *Directory Administrators should never assign more than one to a user.*

In addition to the security roles that provide access to the EDW, there is the security role that provides access to the Warehouse File Exchange drop box. The Data Warehouse File

¹ National Forum on Education Statistics, Forum Guide to Protecting the Privacy of Student Information: State and Local Education Agencies, NCES. Washington, DC: 2004.
<http://nces.ed.gov/pubs2004/2004330.pdf>

Exchange Drop Box role is only available for district personnel and should be assigned to those individuals who will be uploading files such as the student claiming file (see Chapter 3, *Basic Access*) or the data extract files described in Chapter 5, *Advanced Access*. The Data Warehouse File Exchange Drop Box role should be assigned in addition to security role 210 (for student claiming) or security role 209 (for uploading extracts of local data).

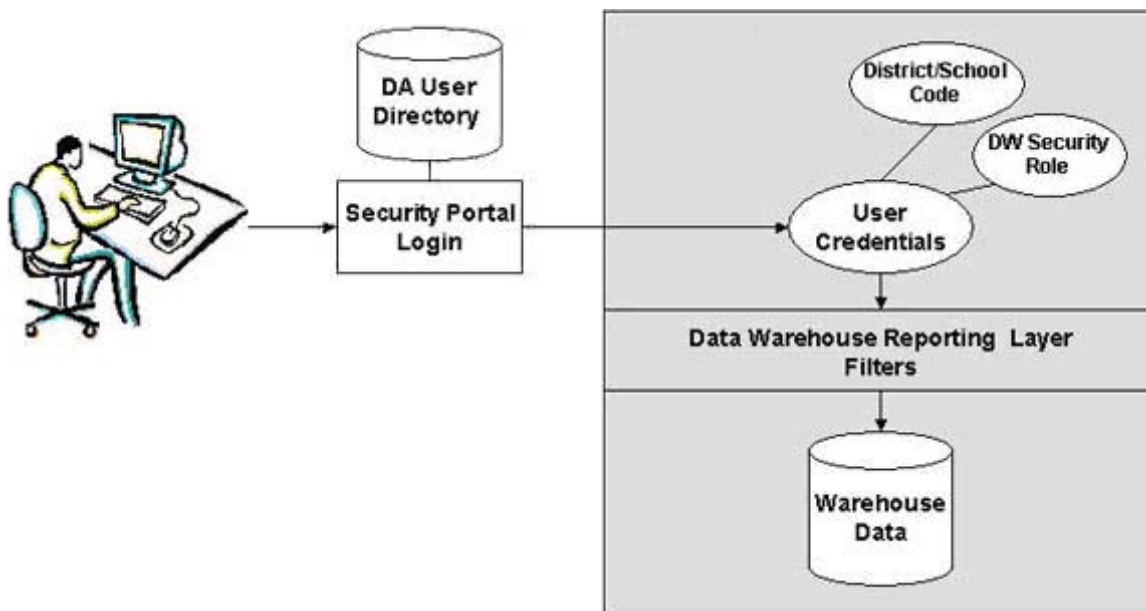


Figure 1 – User Credentials and EDW Data Access

District Data Access Policy

To ensure that confidential data, including data on individual students, is not created, collected, stored, maintained, or disseminated from the Education Data Warehouse in violation of state and federal laws and is not used for unauthorized purposes, school districts shall adopt policies governing access and confidentiality of data maintained in the EDW. Authorized local personnel must participate in training and comply with locally designed confidentiality policies and practices.

For additional information, see Appendix A, *Statewide Education Data Warehouse Policy Statement* available on the Department's [EDW homepage](#).

Training District Users

The Department and grantee districts recently contracted with Public Consulting Group (PCG) to develop a curriculum for training Education Data Warehouse users. Six three-hour courses were developed, piloted, revised, and the final versions posted in the Education Data Warehouse on the security portal. (These documents are not available for use by the general public.) All the materials needed to deliver these courses are available to districts, including PowerPoint presentations, handbooks, tips for the instructors, and printing instructions.

In addition, the Department is preparing a list of approved vendors to deliver the training although districts can choose to have their own personnel deliver the trainings if they

believe them qualified. The approved vendor list will be posted to the [EDW homepage](#) on the Department's public website when it becomes available.

EDW Training Curriculum

The six course curriculum is as follows:

DW101: Introduction to the Data Warehouse

- Inquiry-driven approach to analyzing data
- Functions and benefits of a data warehouse
- Different types and uses of data displays
- Logging on to and navigating the Education Data Warehouse
- Creating folders and defining starting points

DW102: Understanding MCAS Reporting

- Appropriate uses of different types of assessments
- Purposes of the MCAS
- Assessment terms and concepts
- Structure and format of various MCAS reports
- Drawing appropriate conclusions from MCAS reports

DW201: Informing Instruction with Data

- Inquiry-driven approach to analyzing data
- Accessing MCAS pre-defined reports
- Using distracters to identify specific learning needs
- Analyzing open response and short answer items
- Diagnosing learning needs of classes, sections, and individual students
- Action planning

DW202: Multi-Dimensional Analysis

- Inquiry-driven approach to analyzing data
- Basic cube navigation and functions
- Types of charts and graphs available in cubes
- Using dimensions and measures
- Well-designed and thorough data displays
- Designing useful and appropriate data displays

DW301: Report Builder I

- Security roles and reporting packages
- Well-designed and thorough data displays
- Basic features of Report Studio
- Building three basic report types (List, Crosstab, and Chart)
- Filter expressions
- Modifying existing predefined reports

DW302: Report Builder II

- Security roles and reporting packages
- Query calculations
- Report expressions
- Suppressing small cells using conditional formatting
- Building prompt pages

The Department cannot overemphasize the importance of EDW training for district users. The Education Data Warehouse is an excellent tool that facilitates data analysis, but it alone will not ensure successful data use. District users must learn to sort through the wealth of information now available to them and learn how to ask the questions that will provide the focus for their EDW usage. The information covered in courses 101 through 201 should be mandatory for all users. The 202 course should be mandatory for all users with cube access. The 301 and 302 courses should be considered preliminary training for report authors. Report Studio is a powerful but complex tool and additional training is recommended.