SLDS Spotlight

Privacy Classifications for Washington's Data

Introduction

States are increasingly under pressure to balance privacy concerns with the need to collect education data. Much of this pressure has arisen based on the sheer breadth of information available and the heightened sensitivity of education data. But not all data are created equal.

The Family Educational Rights and Privacy Act[1] (FERPA) establishes that educational records defined as "directory information" can be disclosed without consent from students or their parents. Directory information is defined by districts and may include data such as student name, address, date of birth, grade level, enrollment status, dates of attendance, and participation in athletics. A complete list of items that can be classified as directory information can be found in §99.3 of FERPA. Districts have the ability to adopt a limited directory information policy that limits types of information and even limits who has access to that information. Other information collected about a student can be considered private and likely cannot be disclosed without meeting one of several conditions.

Washington is one of several states that take data privacy a step further and establish their own restrictions and data classifications in addition to what is prescribed by FERPA. This brief details how the Washington Office of Superintendent of Public Instruction (OSPI) classified its educational records according to state policy and how the Common Education Data Standards (CEDS) and the CEDS tools assisted in that process.

Data Classification

In the state of Washington, the Office of the Chief Information Officer (OCIO) is responsible for establishing statewide technology policy and standards. Under *Policy 141—Securing Information Technology Assets,*[2] the OCIO is authorized to establish categories for data classification and to instruct agencies to classify their data into one of four categories:

Category 1: Public Information
Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

Category 2: Sensitive Information
Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

[1] Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99, *http://tinyurl.com/kwu64xz*

[2] See Section 4.1, Data Classification, of the Washington OCIO Policy 141.10, Securing Information Technology Assets Standards, *https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets.*

This product of the Institute of Education Sciences (IES) SLDS Grant Program was developed with the help of knowledgeable staff from state education agencies and partner organizations. The information presented does not necessarily represent the opinions of the IES SLDS Grant Program. We thank the following people for their valuable contributions:

Representatives from
Washington State

Kathy Gosa
SLDS Grant Program State Support Team

Bill Huennekens
SLDS Grant Program State Support Team

For more information on the IES SLDS Grant Program or for support with system development, please visit http://nces.ed.gov/programs/SLDS.

ies NATIONAL CENTER FOR EDUCATION STATISTICS
Institute of Education Sciences

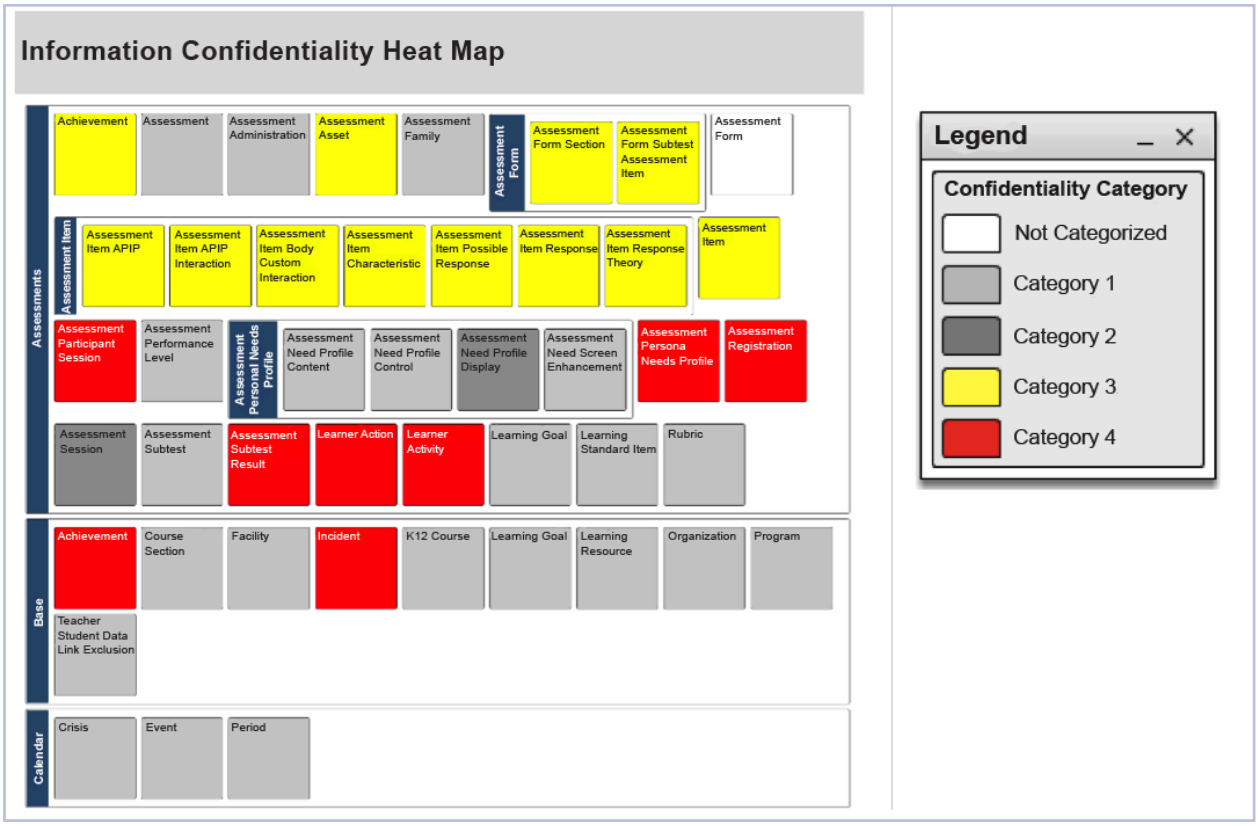

Figure 1.Washington's Information Confidentiality Heat Map

Category 3: Confidential Information
Confidential information is information that is specifically protected from disclosure by law. It may include but is not limited to:

a. Personal information about individuals, regardless of how that information is obtained.
b. Information concerning employee personnel records.
c. Information regarding IT infrastructure and security of computer and telecommunications systems.

Category 4: Confidential Information Requiring Special Handling
Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Classifying Education Records

OSPI's student-level data collection for its statewide longitudinal data system (SLDS) is the Comprehensive Education Data and Research System (CEDARS). Since data within CEDARS are used for various purposes such as accountability, answering policy questions, ED*Facts* reporting, and research, it is important that OSPI categorize all of its data according to the OCIO's policy. Washington was already using CEDS tools for a multitude of purposes and determined that the categorization process could be completed within CEDS Connect.[3] Then OSPI could easily apply its Align map for CEDARS to see how the privacy categories apply to each data element.

Step 1: Applying the Categories to CEDS Elements
To begin this process, OSPI data staff first reviewed the K12 domain of the CEDS Domain-Entity Schema (DES). For each entity, category, and subcategory of data elements within CEDS, staff members determined which of the OCIO categories was most appropriate and created a heat map of the elements color-coded by OCIO category (see figure 1).

The types of education data that fall within Category 1 (Public Information) include information such as school directory information, facility information, K12 course information, assessment performance levels, and the school calendar. At first glance, many of these types of data elements may appear to be private information. However, these elements are not linked to student information and contain only basic descriptive information such as a course name or course time. Mixing data across privacy categories will be discussed in Step 3: Mixing Data from Multiple Categories.

[3] CEDS tools can be found at *https://ceds.ed.gov/*

The types of data that fall within Category 2 (Sensitive Information) include information such as course section enrollment, and K12 staff address and telephone number. These elements are not private, but they should not be publicly disclosed. They should generally only be disclosed based on a specific request.

Category 3 (Confidential Information) generally consists of information related to assessments. The information that was assigned to this category includes items such as assessment item characteristic, assessment item response, assessment form section, and assessment asset. This information is not generally subject to disclosure as it could damage the validity of the assessment.

Category 4 (Confidential Information Requiring Special Handling) contains the most protected information. This is the information that must be kept private and not be disclosed without special permission. As expected, much of the information contained in Category 4 is about individual K12 students. This includes a student's disability status, transcript, discipline, and special programs information. While student address and phone number are considered directory information according to FERPA, and are therefore not protected when provided alone, they fall under Category 4 because they are frequently linked with other student data that render them private.

Step 2: Applying the Categories to Washington's SLDS

Once the entities, categories, and subcategories of the CEDS K12 domain elements were classified according to the OCIO's privacy classification, OSPI data staff needed to apply those classifications to the state's own data. Using the CEDS Connect tool, staff members developed a Connection for each privacy classification. Within each Connection, they then selected all elements from the appropriate CEDS entities, categories, and subcategories assigned to that privacy level.

Through previous efforts, OSPI had created a map in CEDS Align linking its CEDARS data dictionary to CEDS elements. With this map, data staff were able to identify which elements in the CEDARS data dictionary fall into each OCIO category by using the myConnect tool. See figure 2.

Washington's Connection, *Data Classification based on the sensitivity of the data – Category 1*, includes all elements from CEDS' K12 School and Calendar categories, as well as specific sections of the LEA category (Accountability and Address). It also includes elements from other CEDS categories.

https://ceds.ed.gov/connectReport.aspx?uid=764

Figure 2. Partial screenshot of Washington's CEDS Connection, *Data Classification based on the sensitivity of data - Category 2*

The CEDS entities, categories, and subcategories rarely change. By using CEDS to classify privacy levels, OSPI can easily see in its own data system how public or private the data should be and the security that needs to be applied when staff throughout the agency has access to the data.

Step 3: Mixing Data from Multiple Categories

Because some data elements are more confidential and require greater security than others, it is important to consider the mixing of data when deciding what information can be disclosed and what information needs to be de-identified. When data are combined across privacy categories, the category with the highest level of privacy takes precedence. For example, when data from Category 1 are combined with data from Category 4, the resulting dataset should be considered Category 4.

To demonstrate this concept, Washington developed a CEDS Connection titled *Data Mixing: NSLA – Free and Reduced Lunch Eligibility*. This Connection specifies that free and reduced lunch eligibility is protected information under the National School Lunch Act. Because Washington has built and published this Connection on the CEDS website, staff members are able to quickly see which related data elements need to remain private. If there is turnover among OSPI staff, new staff members can more easily understand the rules and regulations concerning disclosure of free and reduced lunch eligibility data.

Replicating the Process

Washington has established the process for classifying its data according to privacy levels established by the state CIO. Other state education agencies can benefit from Washington's process by replicating it for their own use. States can either use Washington's privacy levels or they can copy the information to a new Connection and modify it for their own needs. Several states, including California, are exploring how they can replicate the process for their own data systems.

If your state is interested in replicating or in learning more about Washington's data privacy classification process, please contact the State Support Team at *support@slds-sst.org*.

Tools to Solve Problems

CEDS has tools that can assist with large and small tasks around data management. Washington was one of the first states to align its student information system, CEDARS, to CEDS. When the alignment was done, Washington envisioned using the CEDS mappings to help train new hires about its data.

Until it was presented with the challenge to comply with the OCIO policy, the state had not considered using CEDS to help it address privacy levels for the data. OSPI data staff recognized they could capitalize on work already done through their alignment to CEDS and implement a solution by using additional CEDS tools.

Common Education Data Standards (CEDS) Tools

CEDS tools are available to anyone at no cost. Information published by state education agencies and other organizations—including Washington's Connections and Align maps—are available in the Tools section of the CEDS website without a user account. However, if an agency wishes to create its own Connection and/or Align map, a user account simply requires a name and email address. Once logged in, users have access to an additional set of features that will help manage their data.

The table below highlights the CEDS tools utilized by Washington State. For more information on how to use these tools, contact your State Support Team member or view tutorials available at *http://ceds.ed.gov*.

align A tool containing information on **what** data are being collected	• Upload all or part of a data dictionary • Align the data dictionary to CEDS • Compare the aligned "map" to other maps in your own systems or other systems • Share your map with others • Use the reports feature to find other maps aligned to elements of interest
eConnect A tool containing information on **how** to use data being collected	• Connections define/operationalize metrics, policy questions, and accountability requirements • View published Connections to see how others answered the same question • Provide feedback on Connections to start a dialogue about a topic • Use the reports feature to see an exhaustive list of elements necessary across a set of Connections or to find all Connections using a specific set of elements
myConnect A tool marrying **how** to use the data with **what** is being collected	• Use myConnect to find out which elements in your system can be used to do an analysis defined in a Connection. • You must have either a published map or a published Connection to use this feature.

Additional Resources

Common Education Data Standards (CEDS)
https://ceds.ed.gov/Default.aspx

CEDS and SLDS—Aligning Efforts: SLDS Issue Brief
https://slds.grads360.org/#communities/pdc/documents/5232

Washington Office of Superintendent of Public Instruction
http://www.k12.wa.us/