	POLICY # 13-02	STATUS:	ISSUED: October 2013	LAST REVISED:	PAGE: 1 of 3
	Office of Data & Analysis, Research				
RHODE ISLAND DEPARTMENT OF ELEMENTARY AND SECONDARY EDUCATION	**TITLE:** Data Access and Management Policy: Student Data				

The Rhode Island Department of Elementary and Secondary Education ("RIDE" or "the Department") recognizes that the federal *Family Educational Rights and Privacy Act* (FERPA) (20 U.S.C. 1232 (g)) and the Act's associated regulations (34 C.F.R. 99.1 *et seq*.) provide privacy protection for student records, including those maintained by RIDE. (See, 34 C.F.R. 99.1 (2) & 34 C.F.R. 99.10). The analogous *Rhode Island Educational Records Bill of Rights Act* (R.I.G.L. 16-71-1, et seq.) provides similar protection to student records. RIDE further observes that Rhode Island's *Access to Public Records Act* (R.I.G.L. 38-2-2) provides privacy protection to "personal individually -identifiable records otherwise deemed confidential by federal law or regulation, or state law…" The Department believes that clearly enunciated policies are necessary to ensure compliance with applicable State and federal statutes and regulations in order to provide privacy protection to student records.

1.0 Purpose

RIDE manages many student data repositories designed to collect data, store data, provide access to data and compile and report data. The RIDE Director of Data and Analysis is the designated authority to establish and maintain a system of data protections for RIDE's data repositories in accordance with the Family Educational Rights and Privacy Act (FERPA), the Rhode Island Educational Records Bill of Rights Act and other applicable state and federal laws and applicable technical security standards. It is RIDE policy to ensure that all student data in its repositories are securely maintained; to provide safeguards for all personally identifiable information; and, to ensure that data is received, stored and used only in accordance with applicable state and federal laws and regulations.

Use of Student Data at the Local School Level: This policy statement contains information about the procedures that will be used to ensure the confidentiality of student records maintained in RIDE's data repositories. It does not expand or in any way change the allowable uses of student data by staff in local schools in accordance with applicable local, state and federal laws and regulations.

Electronic Protection of Student Identifiers and Information: To protect the privacy of individual student records, a unique number will be assigned to each student whose

information is contained in the RIDE data warehouse. This State Assigned Student Identifier (SASID), which is computer-generated, will not contain any embedded meaning. SASID numbers will be checked for duplicates and then be permanently assigned to the relevant student.

Data Security: RIDE will ensure that student records in its custody are not lost, stolen, vandalized, illegally accessed, or otherwise rendered useless. RIDE will maintain its data on secure server platforms that provide the highest level of security along with backup and disaster recovery capability. In addition, RIDE will utilize automatic encryption and secure socket layer protocols during data transmissions to ensure that data is transferred in a secure manner.

Disclosure of Statistical Data When a Small Number of Students Will Reasonably Lead to the Identification of a Student's Personally Identifiable Information. When a small student population produces statistical cells small enough to permit the identification of individual students, RIDE will not make such student information available.

RIDE Staff Access to Student Records: It is useful to think of a single record of an individual student as a folder that contains many pieces of information, such as name, school building number, gender, or date of birth, etc. These are called fields. Every field in the student information system is assigned an access level between 1 and 3, with Level 1 being the highest level. Access levels 2 and 3 may be authorized by the Division Chief upon recommendation of the employee's supervising Director.

> ***Level 1 Access*** allows read/write access to all records and field in the repositories. This level is only permitted to a minimal number of RIDE-authorized technical staff members who operate or manage the data warehouse or who are responsible for maintaining the accuracy, security, and audit corrections in the performance of their duties. Authorization by the Deputy Commissioner/General Counsel will be required for this level of access.
>
> ***Level 2 Access*** places limits on access to data to RIDE applications that collect and display data. Authorized RIDE staff have access to RIDE applications that display individual level data only if access is necessary to perform a particularized function of their job and is permitted by state and federal law.
>
> ***Level 3 Access*** allows read-only access for viewing standard reports and data tables that are produced and published in aggregated formats. RIDE will block any aggregate results with statistical cells small enough to permit the identification of individual students. This also applies to third party entities and state government agencies that do not have a specific Data Sharing Agreement with RIDE. Data on individual students will not be accessed by anyone at this read-only level.

Intended Use of Data by RIDE Staff: As with any confidential information in the custody of RIDE, the Department will authorize certain personnel to have access to RIDE data 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 and only for the intended purposes of such use. Authorizations for access by Department of Elementary and Secondary Education personnel shall include approval as articulated in Section 3, Restricted Data Use, of this policy.

Access to RIDE applications for RIDE staff is granted by the Deputy Commissioner / General Counsel. Once a user is given access to a specific application, they will have access to student level data. Depending on the level of access and the application, the individual level data may be filtered by district, school, class, grade, etc. Depending on the level of access and the application, the user accessing the application may have the ability to add new data, edit existing data or delete data.