

Kentucky Department of Education (KDE)



Data Access Policy

If you have questions about this document, contact
KDE's Division of Enterprise Data 502-564-2020

The Kentucky Department of Education does not discriminate on the basis of race, color, national origin, sex disability, or age in its programs and activities. The following person has been designated to handle inquiries regarding the non-discrimination policies – KDE General Counsel.

Policy Type: Data	Title: Data Access Policy
Policy Number: 0003	Effective Date: January 1, 2012



Kentucky Department of Education – Data Access Policy

<p>Responsible Party for Policy Compliance: Associate Commissioners, Division Directors, Branch Managers, Data Managers and Data Stewards</p>	<p>Applicability: (personnel complying with policy) KDE, Schools and Districts</p>
---	---

REVISION HISTORY:

The following is the revision history for this policy.

Version	Date of Issue	Author(s)	Brief Description of Revision
1.0	12/31/12	DeDe Conner	Approved by Core Process Team
1.1	02/05/13	DeDe Conner	Updated per OGC edits.



Table of Contents

- I. **Policy Statement**
- II. **Purpose**
- III. **Scope of Policy**
- IV. **Definitions**
- V. **Information Collected and Maintained**
- VI. **Measures to Maintain Confidentiality**
- VII. **De-Identification of Student-Level**
- VIII. **Suppression Rules**
- IX. **Data Security**
- X. **Data Access**
- XI. **Training Needs**
- XII. **Responsibility for Process**
- XIII. **Process for Handling Information Requests from Researchers**
- XIV. **Record of Access**
- XV. **Destruction of Data**
- XVI. **Penalties for Violation of Data Use**



I. POLICY STATEMENT

The Kentucky Department of Education (KDE) collects education records from local schools and districts in accordance with federal and state laws and regulations. Data is utilized for federal and state reporting, funding calculations, and research. KDE does not permit access to, or the disclosure of, student education records or personally-identifiable information contained therein except for purposes authorized under the Family Educational Rights and Privacy Act (FERPA).

Furthermore, KDE protects information obtained through the USDA free/reduced lunch program. Data collected through these measures will not be released except as allowed in 7 C.F.R.245.6 .

II. PURPOSE

This policy establishes the procedures and protocols for collecting, maintaining, disclosing, and disposing of confidential data records, including data collections containing personally-identifiable information about students, personnel, and free and reduced lunch programs. It is intended to be consistent with the disclosure provisions of the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and the National School Lunch Act, 7 CFR 245.6.

III. SCOPE OF POLICY

These policies and procedures apply to all employees, contractors and 18a, of the Kentucky Department of Education (KDE) and are applicable to other entities requesting access to confidential, sensitive, or restricted information.

Related policies, laws, operating procedures and other documents which contain directives that apply to agency confidential, sensitive and restricted enterprise information include:

- Family Educational Rights and Privacy Act (FERPA) 34 CFR, Part 99 located at <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- USDA Food and Nutrition Service National School Lunch Program at <http://www.fns.usda.gov/cnd/lunch/> KDE Statement of Non-Disclosure(s) and KDE Non-Disclosure for Free and Reduced Lunch
- Memorandum of Understanding(s) between KDE and outside agencies or entities.



IV. DEFINITIONS

- A. Authorized Representative refers to any entity or individual designated by a State or local educational authority to conduct any audit or evaluation, or any compliance or enforcement activity in connection with Federal legal requirements that relate to these programs FERPA 34 C.F.R. § 99.3).
- B. Confidentiality refers to how personally identifiable information collected by schools, districts, and agencies is protected and when an individual’s consent is required to disclose.
- C. Data Requirements gives written description of data requirements associated with data request.
- D. Data Collection includes any collection of educational records, which may include data collected in an enterprise-level system (e.g., Student Information System) or through alternate collection means.
- E. Data Request refers to any request made to agency or outside entity for data associated with educational records.
- F. De-identification is a process which renders data safe to utilize and share by removing or obscuring all identifying fields such as name or identification numbers, thus making it very difficult to identify an individual based on a combination of variables, KDE will employ a set of data de-identification rules.
- G. Directory Information refers to information from student education records that may be disclosed, without consent. "Directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance are included. However, schools must tell parents and eligible students about directory information and allow parents/guardians and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.
- H. Disclosure or Disclose means to permit access to or the release, transfer, or other communication of personally identifiable information contained in education records by any means, including oral, written or electronic means (internally or externally).



Kentucky Department of Education – Data Access Policy

- I. Education Record describes any information or data recorded in any medium, including but not limited to handwriting, print, system, which contain information directly related to a student, school or district (including personnel records) and which are maintained by an educational agency or institution or a person acting for such agency or institution. See 20 U.S.C. 1232g(a)(4)(A); 34 C.F.R. 99.3.

- J. Educational Programs refers to any program under the provision of education including but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency, KDE, or institution (FERPA regulations 34 C.F.R. § 99.3).

- K. Eligible Student refers to a student under the age of 18 who is enrolled in a Kentucky post-secondary educational institution or one who is over the age of 18. An eligible student has the right to access to his or her education records, the right to seek to have the records amended, the right to control the disclosure of personally identifiable information from the records, and the right to file a complaint with the U.S. Department of Education. Eligible students will be assigned a unique student identifier number. (FERPA regulation 34 C.F.R 99.3)

- L. Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law designed to protect the privacy of student education records and to allow students, their parents and/or legal guardians' access to the student's educational record.

- M. Free and Reduced Price Lunch data refers to information collected from the application of federal Free and Reduced Meal program and is protected by federal laws and regulation 7 C.F.R. 245.6 which governs its confidentiality and disclosure.

- N. Kentucky Student Information System (KSIS) – authoritative source system at KDE for student level information entered and maintained at schools and districts.

- O. Legitimate Educational Interest, for the purposes of this policy, is an endeavor meant to further the understanding of educational practices, methods, and/or theory that is expected to be analyzed and is: (1) necessary for that school official to perform appropriate tasks that are specified in his or her position description or by a contract agreement; (2) used within the context of official agency or school business and not for purposes extraneous to the official's areas of responsibility or to the agency or school; (3) relevant to the accomplishment of some task or to a determination about the student; and (4) consistent with the purposes for which the data are maintained.



Kentucky Department of Education – Data Access Policy

- P. Linkage consists of the ability to combine educational records through use of common identifiers for the purpose of research or re-identification.
- Q. Memorandum of Understanding, MOU, refers to the data disclosure and confidentiality agreement between the Kentucky Department of Education and the entity requesting data.
- R. P20 Data Collaborative is a joint effort from the Kentucky Department of Education (KDE), the Council on Postsecondary Education (CPE), the Education Professional Standards Board (EPSB), and the Kentucky Education and Workforce Development Cabinet to create a shared data system with pre-school (P), Post-Secondary (20), and workforce data. This system links data together from early childhood, K-12, postsecondary and other sources to allow stakeholders to develop a broader understanding of the implications that programs and policies have on our state.
- S. Personally Identifiable Information (PII) includes the name and address of the student and the student’s family; a personal identifier, such as the student’s Social Security Number, student number, or biometric record; other indirect information, such as the student’s date and place of birth and mother’s maiden name; other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of relevant circumstances, to identify a student with reasonable certainty; and information based on a targeted request.
- T. Privacy defines the right of individuals to have their personal information adequately protected to avoid the potential for harm, embarrassment, inconvenience, and/or unfairness.
- U. Re-disclosure describes the sharing or use of data collection beyond the original, approved, intent.
- V. Security means technical procedures that are implemented to ensure that records are not lost, stolen, vandalized, illegally accessed, or improperly disclosed.
- W. State Student Identification (SSID) Number is a unique number assigned by the Student Information System to track student and education records. It does not contain any series of numbers matching a Social Security number.
- X. Student refers any person who is or has attended a public or accredited non-public school and for whom an educational agency or institution maintains education records. See 34 C.F.R. 99.3.



- Y. Suppression denotes withholding information from publication. Some information is withheld from publication to protect small counts that could lead to a disclosure. Other information is withheld from publication in a table to prevent the calculation of the data based on small counts from the published information; this is known as complementary suppression.
- Z. Vendor-Partner includes any KDE contract holders with access to education records.

V. INFORMATION COLLECTED AND MAINTAINED

KDE collects, through enterprise data systems and other collection methods, education records on Kentucky schools, districts, and students, including:

- A. Personally Identifiable Information which identify each student. These data may include, but are not limited to name, identification number, address, race/ethnicity, gender, date of birth, place of birth, social security number, economic status, free and reduced price meal plan records;
- B. Participatory data including attendance, student progress, grade level completed, school attended, academic work completed, assessments, and date of graduation. This includes performance data from multiple sources, such as the statewide assessment, Advanced Placement, ACT and SAT;
- C. Program data including eligibility for special education, special education services provided to the student, eligibility for other compensatory programs and other special program services provided to the student.
- D. School and district data that includes information on school facilities, teachers, teacher of record, courses and rosters, administrators and staff.
- E. Financial data is collected at the state and local school districts levels in the way of budgets and expenditures (annual submission).

Education records may be maintained in one or more data systems. All systems and collections shall be subject to this policy.



VI. MEASURES TO MAINTAIN CONFIDENTIALITY

KDE shall utilize various procedures and security measures to ensure the confidentiality of education records. These procedures include assignment of a unique identifier to each student, a system of restricted access to data, and statistical cutoff procedures.

- A. A unique State Student Identification number (SSID) is assigned to each Kentucky student. The student ID is computer-generated and contains no embedded meaning. The student locator tool in the KSIS system assigns a unique ID and is used to identify transfer students to avoid creating multiple IDs for a single student.
- B. Security protocols limit who has access to the data and for what purposes.
- C. Statistical cutoff procedures (suppression rules) are utilized to prevent student inference in aggregate-level reports.
- D. All KDE employees, contractors and vendor-partners must abide by FERPA requirements, National School Lunch requirements and this Data Access Policy.
- E. KDE shall maintain a current listing of agency personnel who have access to personally-identifiable student information through authentication and internal links.
- F. Confidential or identifiable student-level data should be communicated or transferred electronically to external entities through a secure FTP site. Student level data should be password protected prior to any exchange through email or alternative transfer method. The password should not be included in the email with the student-level data, it must be provided through a separate communication.
- G. De-identification rules as established within this policy must be followed to ensure confidentiality of data shared for research purposes.
- H. Other safeguards -- All agency employees, agents of the KDE, researchers, and other entities with direct access to confidential student information are responsible for protecting the data via the following procedures:
 - Prevent disclosure of data by protecting visibility of reports and computer monitor when displaying and working with confidential information.
 - Workstations must be locked or shutdown when left unattended for any amount of time.
 - Data must be stored in a secure location. Electronic files should be password protected and/or stored in a location only accessible by the authorized entity. Confidential information will not be faxed.



Kentucky Department of Education – Data Access Policy

- When no longer needed, paper reports must be shredded and electronic files must be destroyed.
- Reports, CDs, and/or any other media containing confidential information must be stamped or otherwise marked as confidential prior to being released outside the agency. The envelope containing the information must also indicate that the contents are confidential.
- The envelope containing the information must also indicate that the contents are confidential.

VII. DE-IDENTIFICATION OF DATA

De-identification involves the removal of personally identifying information in order to protect personal privacy. With the exception of disclosure of education records for audits and evaluations and studies as defined by FERPA, data is provided in a de-identified or aggregate form. Social Security numbers, names, date of birth or other identifiable data is excluded. The State Student Identification (SSID) Number can be provided to allow for matching of data records or re-identification but must be excluded from any publically produced reports.

VIII. SUPPRESSION RULES

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.” Consequently, it is the 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. The exceptions to this policy are enrollment counts disaggregated by grade level, and/or gender; which are reportable down to one. Suppression of data in the form of percentages when the percentages are 0 or 100 for any student demographic categories.

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. Internal and external report authors also should be aware of small group suppression rules. Report authors are responsible for ensuring that the Department’s suppression policy is applied appropriately to any reports created.

KDE suppresses counts of less than 10 and counts and percentages that would attribute to entire populations ex: 0 or 100%. KDE abides by and recommends adherence to Privacy Technical Assistance Center, or [PTAC, Technical Briefs](#) for protecting education



Kentucky Department of Education – Data Access Policy

records. In this effort KDE will suppress using reasonable methods to ensure to the greatest extent practicable that PII will not be disclosed.

IX. DATA SECURITY

KDE has measures in place to maintain the security of the records. The procedures used to ensure the privacy and security of computer records include but are not limited to: password applications that restrict access to data elements and files only to those with authorization, frequent password changes to guard against break-ins, the use of encryption, and monitoring of user access to the secured files.

KDE defines Data Tiers (see Enclosed) to help define sensitivity of data and assist employees with making informed decisions before releasing confidential data.

X. DATA ACCESS

This section describes the conditions under which the KDE will release confidential information. Confidentiality refers to a person's obligation not to disclose or transmit information to unauthorized parties. The requesting entity or individual must sign and have an approved KDE a Memorandum of Understanding, MOU, as appropriate before any data will be released. Authorization must be evaluated annually to ensure access to the data is still required. Use of data is only for purposes as defined in the signed MOU.

Intentional violations of this policy by a KDE employee may result in formal disciplinary action, up to and including termination (e.g. denial of access to sensitive data, and revocation of network access privileges).

The entities to which information may be released and the conditions of the release are listed for each entity below.

- 1) **KDE Staff** –All KDE staff must sign Non-Disclosure agreements at the time of employment including one for FERPA and one for Free and Reduced Price Lunch data. KDE staff members who have a need to access confidential student-level information are permitted access through system access protocols established and maintained by KDE system administrators. Supervisors (branch manager level or above) must sign to indicate that the staff person needs access to this information in the performance of his or her assigned duties and responsibilities. Supervisors will ensure that the appropriate safeguards are instituted to protect the confidentiality of student information and that the staff person has received appropriate training. KDE staff may not access agency information for personal purposes (for example, research for a dissertation). Employees must maintain the



Kentucky Department of Education – Data Access Policy

confidentiality of all education records. Data will be destroyed in accordance with State's record retention policy.

- 2) **Public** - The KDE may disclose, without consent, student information in aggregate form which is not easily traceable to a student. Public access is limited to aggregate level reports. Suppression rules set forth in this policy are adhered to for all public reporting. Non-confidential data is Tier 1 data and available to anyone through the KDE Open House website at <http://openhouse.education.ky.gov>.
- 3) **Parents and Students** are provided access to their education records through the KSIS portal. Any additional request for access to records must be made in writing to the applicable school or district.
- 4) **Research** - KDE may disclose confidential, personally-identifiable information of students to individuals and/or organizations for research and analysis purposes to improve instruction in public schools. Disclosure is authorized under the FERPA Studies Exception. Any such disclosure shall be made only if (1) the conditions in FERPA regulation 34 CFR 99.31(a) (6) are met; (2) The request for data sharing must be approved by KDE with a Memorandum of Understanding, MOU for Studies Exception, signed to ensure compliance with FERPA regulations, National School Lunch Requirements and KDE policies; (3) Requester agrees to return or destroy education records at completion of research use. (4) Researcher understands associated penalties for violation of data privacy, use or re-disclosure.
- 5) **P20 Data Collaborative** - personally identifiable data is provided to the P20 Collaborative per the MOU between agencies.
- 6) **Other Entities** – All other entities will be denied access to confidential information unless the entity is using the data to develop, validate, or administer predictive tests or improve instruction as defined in FERPA 34 C.F.R. § 99.31(a)(6). Agents of the Comptroller General of the United States, the Secretary of the U.S. Department of Education, or state and local educational authorities will be provided access to the data provided the disclosure is in the course of an audit, evaluation, compliance, or enforcement proceeding as defined in FERPA 34 C.F.R. §§ 99.31(a)(3), 99.35. The information will be protected to shield personal identification of students by others and the information will be destroyed when no longer needed. The KDE shall enter into an MOU with any entity it designates as its “authorized representative” under 34 C.F.R. 99.31.



Kentucky Department of Education – Data Access Policy

The KDE will disclose education records, without consent, to the parties listed immediately below under the following conditions:

- other schools when a student is transferring in order to facilitate school enrollment;
- appropriate officials in cases of health and safety emergencies;
- KDE supported systems in respect of sharing authoritative source data between systems.

XI. TRAINING NEEDS

All KDE staff shall be made aware of the Data Access Policy and will receive subsequent information through newsletter articles, e-mail messages, and/or training classes.

XII. RESPONSIBILITY FOR PROCESS

The Office of Knowledge Information and Data Systems (KIDS) Division of Enterprise Data at the KDE is primarily responsible for data requests. Data requests must be approved by the Data Policy Committee.

XIII. PROCESS FOR HANDLING INFORMATION REQUESTS

Utilizing the data request process outlined on Open House, complete data request template with associated requirements. Submit completed request form as specified.

A. Data requests for specific information will be honored only if one of the following is true:

- 1) The material requested has already been published or collected and can easily be put into a distribution format that protects confidential information. In these cases, information can be provided without a review by the KDE Data Policy Committee.
- 2) The requestor completes the process for conducting research with KDE data and has his/her proposal approved by the KDE Data Policy Committee.

B. Proposals submitted to the KDE Data Policy Committee will be subject to the following:

- 1) Proposals should be forwarded to appropriate staff within the KDE for their comments and recommendations prior to submitting to the Committee. Information provided by the KDE staff will be considered in the proposal review.
- 2) Research proposals that fall under the KDE's primary mission or strategic initiatives will receive first priority.



Kentucky Department of Education – Data Access Policy

- 3) The KDE staff resources may limit the number of requests that can be honored during a fiscal year. Thus, some worthy studies that receive approval may need to be postponed until KDE resources are available.
- 4) The KDE Data Policy Committee will meet as needed to consider proposals.
- 5) Researchers will provide a copy of products resulting from the research (e.g., publication, report, and book) to the KDE Data Policy Committee.

XIV. RECORD OF ACCESS

In compliance with FERPA guidelines, KDE shall maintain a record indicating the name of any individual or organization external to KDE that requests and is allowed access to educational records. The record of access shall indicate the interest such person or organization had in obtaining the information, as well as the date the requested data were disclosed. See 20 U.S.C. 1232g (b) (4); 20 U.S.C. 1232g (j) (4).

XV. DESTRUCTION OF DATA

Any entity receiving personally-identifiable information must destroy such information when it is no longer needed for the purpose specified in the request for disclosure. The manner of destruction shall protect the confidentiality of the information and must be done at the conclusion of the intended purpose.

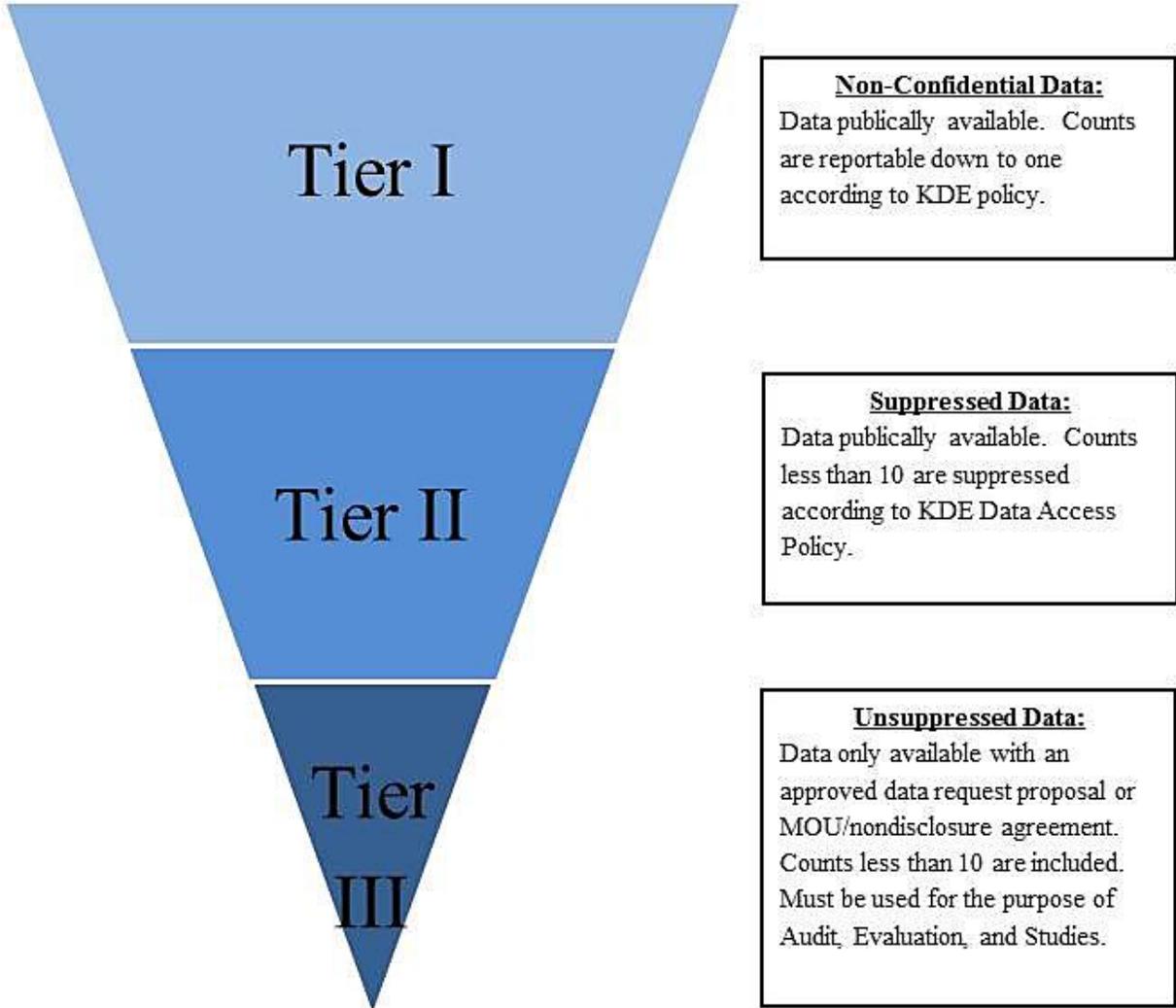
XVI. PENALTIES FOR VIOLATION OF DATA USE

Enforcement penalties for violation of data privacy security, unauthorized disclosure or re-disclosure will result in loss of access to education records.

XVII. SUPPLEMENTARY INFORMATION

The National Center for Education Statistics' [Privacy Technical Assistance Center](#) has tools available to help education stakeholders learn more about data privacy, confidentiality, and security practices related to student-level data sharing. A series of [technical briefs](#) are available to assist states. By reference, KDE incorporates these guidelines.

Data Tiers Defined





Kentucky Department of Education – Data Access Policy

DATA TIERS FOR EXTERNAL RELEASE OF DATA KDE Student Records Confidentiality Examples of Data Request <small>** These are examples and not meant to be all-inclusive.</small>	Available on Web	Suppressed	Unsuppressed	Aggregate	Approved Research Proposal Required
--	------------------	------------	--------------	-----------	-------------------------------------

Tier I	Aggregate-level counts by school or district without identifiable attributes such as gender, race or other characteristics, such as:	X		X	X	
	• School & District Contact Information	X		X	X	
	• Free & Reduced Counts	X		X	X	
	• Enrollment by district, school, and grade	X		X	X	
	• Enrollment by system	X		X	X	
	• Special Education Students by School	X		X	X	
	• Dropout, Retention, and Transition Rates by School	X		X	X	
	• SEEK Funds by district	X		X	X	
	• Tier I, II & III Schools, Focus Schools, and Priority Schools	X				
• School Accountability System Measures at State, District, and School Levels	X					
Tier II	Tier I Data with additional breakout by gender, ethnicity, or other attribute that could lead to identification:		X		X	
	• State Assessments: K-PREP and EPAS	X	X		X	
	• School Report Card	X	X		X	
	• Safe Schools (district/aggregate)	X	X		X	
	• Open House Data	X	X		X	
Tier III	Tier I or II Student Level detail with personally identifiable characteristics for purposes of research or program accountability that is not de-identified or suppressed					X
	• Safe Schools Behavior data (student level)					X
	• P20 Data Sets					X