Data Collection, Access, and Use Policy (0003)

Policy Type: **Data**	Title: **Data Collection, Access and Use Policy**
Policy Number: **0003**	Effective Date: **January 1, 2012**
Responsible Party for Policy Compliance: **Associate Commissioners, Division Directors, Branch Managers, Data Stewards and Data Controllers**	Applicability: (personnel complying with policy) **KDE Agency and Third-Party Vendors/Contractors involved with KDE data systems**

History and Approval

Version	Date of Issue/Update	Author(s)	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.
2.0	9/10/15	Linda Burton	Major revision

Approval	Date
Data Governance Committee - Review	8/24/2015
Core Process Team - Review	8/27/2015
Chief Information Officer/KIDS Associate Commissioner - Approval	9/10/2015

Authority

The Data Governance Committee will review the Data Collection, Access, and Use Policy annually; when there is a change to a data collection, access or use activity; and upon request by the Knowledge and Information Core Process Team (Core Process Team). If, at any time, a portion of this policy conflicts with a state law or regulation that has jurisdiction over the Kentucky Department of Education (KDE) and/or Kentucky school districts, the law or regulation shall take precedence over that portion of the policy and the rest of the policy shall remain in effect.

The KDE Data Governance Committee has responsibility for establishing and promoting policies (appendix N-1, KDE Data Governance Policy). The committee operates under the authority of the KDE chief information officer (CIO) and the Knowledge and Information Core Process Team). The CIO and Core Process Team review and make determinations on implementation of data policies and policy updates proposed by the Data Governance Committee.

If you have questions or comments regarding this document, contact the KDE chief data officer at 502-564-2020.

Purpose and Scope

The Kentucky Department of Education (KDE) is responsible for management of the state's education information systems and adheres to the confidentiality requirements of federal and state laws including, but not limited to the Family Educational Rights and Privacy Act (FERPA), the Individuals with Disabilities Education Act (IDEA), the Protection of Pupil Rights Amendment (PPRA), and the National School Lunch Act (NSLA). See appendix O for a summary of key state and federal laws regarding education and other personal information.)

The purpose of this policy is to ensure efficient utilization of state and local resources, consistent use of data quality controls, preservation and protection of individual and collective privacy rights, and confidentiality and security of collected data. This policy establishes protocols for collecting, accessing, and using enterprise data including, but not limited to, data collections containing confidential and personally identifiable information (PII).

The provisions of this policy apply to all KDE agency personnel, including employees, temporary staff, contractors and third-party vendors involved with KDE data systems. All KDE personnel and other parties involved with KDE data systems shall support, participate in and promote KDE's Data Collection, Access and Use Policy. Education records and other records containing personally identifiable information may be maintained in one or more data systems; however, all KDE information systems and collections shall be subject to this policy.

Local education agency (LEA) staff may refer to this document for an overview of KDE's statewide data policy and as a reference for local data policy.

Contents

History and Approval i
Authority i
Purpose and Scope ii
Chapter 1. Data Collection 1
Enterprise Information Systems 1
Authoritative Source 1
Change Control 1
Quality Control 2
Enterprise Data Dictionary 2
Data Collection Calendar 2
Data Standards 2
Chapter 2. Data Access 3
LEA data access 3
Internal data access 3
Parent/student access 4
Open records 4
Judicial Order or Lawfully Issued Subpoena 4
Disaster, Health or Safety Emergency 4
Public Data Access 5
De-Identification of Data 5
Cell Suppression 5
Open House 5
Chapter 3. Data Use 7
LEA Data Use 7
KDE Data Use 7
Federal Data Use 7
External Data Use 7
Studies 8

Audit/Evaluation 8
Record of Disclosure 9
Retention 9
Destruction of Data 9
Appendices 10
A. Acronym Reference Guide 10
B. Definitions 10
C. Data Controllers/Data Governance Committee 10
D. Data Guidelines and Procedures 10
1. Data Breach 10
2. Data Collection Request Form (KDE use only) 10
3. Enterprise Data Dictionary 10
4. Data Collection Calendar (available soon) 10
5. Data Standards 10
6. Data Security Training Plan (available soon) 10
7. Data Security Video Series 10
8. External Data Use 10
9. Destruction of Data 10
10. System Access Protocols (available soon) 10
E. Data Governance Organizational Chart 10
F. Data Requests 10
G. Data Request Form 10
H. Data Stewards 10
I. Employee Affidavit of Nondisclosure 10
J. FERPA Exceptions Summary 10
K. MOU – Studies 10
L. MOU – Audit/Evaluation 10
M. State Government Records Retention Schedules 10
N. Data Policies 10
1. Data Governance 11

2. Data Collection, Access and Use – Work in Process 11
3. Data Security Policy - Work in Process 11
O. Summary of key state and federal laws regarding education and other personal information 11
P. United States Department of Education (USDOE) Ed facts 11
Q. Other Resources and Best Practices 11
1. Privacy Technical Assistance Center (PTAC) 11
2. Data Quality Campaign 11
3. National Forum on Education Statistics 11
R. Data Definitions 12

Chapter 1. Data Collection

Schools collect information such as grades, program participation, demographics, and attendance. As originators of most education data, schools and other local education agencies (LEAs) are responsible for the accuracy, quality, completeness, and timeliness of entering their data into the appropriate statewide enterprise information system. As data is collected, information is available to authorized LEA and KDE users through the enterprise level systems.

Enterprise Information Systems

LEAs and KDE use statewide enterprise information systems to collect a variety of data on students, educators, facilities, and finances. Kentucky education data systems are intended to support better decision-making for improving the performance of students and schools reduce reporting burdens, help facilitate the entry of students into new schools and ensure that timely, high quality data are available for reporting, audits and evaluation. The Systems Launchpad provides information about Kentucky's statewide educational systems.

To reduce the risk of unauthorized disclosure of personal identity, students, faculty and staff are assigned a system identification number for identification within most systems. An individual's Social Security Number (SSN) is collected and used where required by law or for specific purposes. KDE allows limited access to and use of SSNs. KDE leadership must approve state-level access to SSN data.

The Infinite Campus enterprise information system assigns each student a Statewide Student Identifier (SSID), which is a unique, non-personally-identifiable number at the time the student is first enrolled into a Kentucky public PK–12 educational program. SSIDs are used to maintain data on individual students, such as linking students to statewide assessment scores and tracking students in and out of LEAs in order to determine more accurate dropout and graduation rates.

The enterprise information systems assign each staff a Person ID or Employee Number, which is a unique, non-personally-identifiable number at the time the first employment record is created. The Person ID or Employee Number can be used within a district as a unique identifier but it is not typically used as a state reporting ID as it is not unique between districts.

Authoritative Source

The Data Governance Committee determines the authoritative source system. To ensure data consistency and integrity, any new data collection, data update or correction should be made through the authoritative source.

Change Control

For any request to add, revise or eliminate a data system, collection, element, field, metadata, or definition, use the KDE Data Collection Request form (appendix D-2). The Data Governance Committee

will review the request to evaluate its impact on KDE and LEAs and, when applicable, will provide LEAs an opportunity for input.

The Data Collection Request form must be complete, including director or associate support, scope, reason/justification, implementation date, supporting law or regulatory requirements and instructions. The request should include a risk analysis describing known or possible risk for not implementing or postponing change; people, groups, organizations affected; and complexity constraints such as a tight implementation window.

Quality Control

Data stewards are responsible for management and oversight of KDE's enterprise data assets to provide high quality data that is easily accessible in a consistent manner. See appendix N-1, KDE Data Governance Policy V1.4 for data stewards' roles and responsibilities.

Enterprise Data Dictionary

The Data Governance Committee will maintain the KDE Enterprise Data Dictionary to ensure that it is accurate, up to date, and available to support agency data collections and data use. The Enterprise Data Dictionary identifies and describes all data elements, contains key metadata and defines the authoritative source. In some cases, the U.S. Department of Education maintains a definition of a required data element; where federal definitions do not exist, a standard definition should be used for comparability of data. The data dictionary will be used to increase understanding of the data elements and to support data quality.

Data Collection Calendar

KDE publishes an annual Data Collection Calendar, which lists the data collections required by state and federal statutes along with timelines for data validation and submissions.

Data Standards

KDE provides KSIS Data Standards to guide LEA staff with data entry to ensure a uniform collection of data. KSIS Data Standards are used to gain an understanding of the data and for clarification on what the data indicate. KDE Data Stewards create and update the KSIS Data Standards as needed. At least annually, each data steward conducts a thorough review to ensure the information is both relevant and current.

Chapter 2. Data Access

Appropriate access to education and other confidential data enables teachers, administrators and policymakers to positively impact individual, district and statewide student achievement and organizational efficiencies. State and federal statutes (appendix O) provide specific protections regarding access to education and other confidential data and are incorporated into local and state policies regarding access to education and other confidential data.

LEA data access

Each LEA determines local policies and procedures regarding access to LEA-level education and other confidential data.

Internal data access

KDE restricts access to confidential data based on job and role-specific needs that correspond to a specific educational or business purpose.

For access to enterprise systems, KDE requires staff, upon employment and as an annual renewal, to sign appropriate access agreements including, but not limited to, the KDE Employee or Contractor General Affidavit of Nondisclosure (appendix I). The Data Governance Committee is responsible for tracking the collection of nondisclosure affidavits for systems users and for revoking access if the condition is not met.

KDE staff who have a need to access confidential student-level information are permitted access through system access protocols established and maintained by KDE system administrators (appendix D-10). Supervisors (branch manager level or above) must approve by signature to indicate that the staff person needs access to this information in the performance of his or her assigned duties and responsibilities. Access to certain data elements, such as Social Security Number, and collections, such as student behavior records, require associate commissioner approval and signature. Supervisors will ensure that the appropriate safeguards are instituted to protect the confidentiality of student/individual information and that the staff person has received appropriate training on measures to safeguard confidential data. KDE staff may not access agency information for personal purposes (e.g., his/her own child's records and research for a dissertation). Employees must maintain the confidentiality of all education or personally identifiable records.

Staff changing their job duties, who still work at KDE, shall have their access and operational privileges reviewed immediately and where required, updated. This review and update will focus equally on eliminating access privileges no longer required as well as providing new/enhanced access privileges required of the user's new job duties. Upon termination of an individual's employment, KDE Human Resources personnel shall notify systems administrators and access will be immediately revoked.

Within a reasonable and appropriate time following their start date and, minimally, on an annual basis thereafter, All KDE personnel will be provided access to KDE Data Security video series with tracking of participation. Other training will be made available to address the pertinent topics according to the agency training plan.

Parent/student access

Parents and students are provided access to their education records through the KSIS portal or associated mobile application. Any request for additional access to records must be made in writing to the applicable school or district. Schools must respond to requests as soon as reasonably possible, but within 45 days.

Open records

The Kentucky Open Records Act (KRS 61.870 to KRS 61.884), or KORA, provides access to public records that, by law, are not exempt from disclosure. For more information on the act, visit the Kentucky Office of the Attorney General Web site at http://ag.ky.gov/opengov.htm. Student records are protected from open records disclosure by the Family Educational Rights and Privacy Act (FERPA). Questions about the application of the Open Records Law to particular types of KDE records may be directed to KDE Chief Legal Counsel, Office of Guiding Services.

Judicial Order or Lawfully Issued Subpoena

FERPA permits disclosure without consent if the disclosure is necessary to comply with a lawfully issued subpoena or judicial order. More often, an LEA would receive such an order; however, the party named in the order must make a reasonable effort to notify the parent or eligible student of the subpoena or judicial order before complying with it in order to allow the parent or eligible student to seek protective action, unless certain exceptions apply. 34 CFR § 99.31(a)(9).

Disaster, Health or Safety Emergency

On a case by case basis, KDE may determine that it is necessary to disclose, without consent, information to appropriate parties to address a disaster or other health or safety emergency (e.g., tornado or fire), if knowledge of that information is necessary to protect the health or safety of the student(s) or other individual(s). Under FERPA, this exception to the general consent requirement is temporally limited to the period of the emergency and generally does not allow for a blanket release of personally identifiable information from the student's education records. KDE must record in the student's education records the significant threat that formed the basis for the disclosure and the parties to whom information was disclosed (appendix O, (34 CFR §§ 99.31(a)(10) and 99.36) and 34 CFR § 99.32(a)(5)).

Typically, law enforcement officials, public health officials, trained medical personnel, and parents (including parents of an eligible student) are the types of appropriate parties to whom information may be disclosed in a health/safety emergency.

Public Data Access

KDE reports timely, actionable, and comprehensible data to promote transparency, strengthen accountability, and ensure that everyone with a stake in education—parents, educators, policymakers, researchers, and members of the public and press—has access to the information needed to make good decisions. This data also demonstrates the value of the enterprise data systems. All data are aggregated and suppressed to protect student privacy.

De-Identification of Data

Specific steps and methods used to de-identify information may vary depending on the circumstances, but should be appropriate to protect the confidentiality of the individuals. De-identification is considered successful when there is no reasonable basis to believe that the remaining information in the records can be used to identify an individual. De-identified data may be shared without the consent required by FERPA (34 CFR §99.30) with any party for any purpose, including parents, general public, and researchers (34 CFR §99.31(b)(1)). These data are typically released in the form of aggregated data (such as tables showing numbers of enrolled students by race, age, and sex) or micro data (such as individual-level student assessment results by grade and school). It is important to note that PII may include not only direct identifiers, such as names, student IDs or social security numbers, but also any other sensitive and non-sensitive information that, alone or combined with other information that is linked or linkable to a specific individual, would allow identification. Therefore, simple removal of direct identifiers from the data to be released DOES NOT constitute adequate de-identification. Properly performed de-identification involves removing or obscuring all identifiable information until all data that can lead to individual identification have been expunged or masked. Further, when making a determination as to whether the data have been sufficiently de-identified, it is necessary to take into consideration cumulative re-identification risk from all previous data releases and other reasonably available information, including publicly available directory information and de-identified data releases from education records as well as other sources. The release of education records that have been de-identified is not considered a “disclosure” under FERPA, since by definition de-identified data do not contain PII that can lead to identification of individual students.

Cell Suppression

KDE suppresses small cell data to ensure that personally identifiable information will not be disclosed. Cell suppression is implemented for public reporting purposes so that no student can be identified by process of elimination where a group may include small numbers of students. No reports are produced with tables containing small cells such that individual students can be identified. KDE abides by and recommends adherence to the Privacy Technical Assistance Center for guidelines and best practices in regards to protecting education records.

Open House

KDE provides Open House as a public one-stop-shop for education data. All data are aggregated and suppressed, where applicable, to protect student privacy.

School Report Card

KDE provides School Report Card information, specific to each school and district that include test performance, teacher qualifications, student safety, parent involvement and much more. The School and District Report Cards were established by statute and regulation (appendix O, KRS 158.6453 and 703 KAR 5:140). Additionally, the report cards incorporate the requirements of the federal No Child Left Behind (NCLB) Act (appendix O).

While the KDE website is the most convenient and inexpensive way for the vast majority of Kentucky parents to receive this information, schools and districts are required, upon request, to print cards for parents lacking Internet access.

Supplemental Data

KDE provides Supplemental Data after publication of the annual School Report Card. Supplemental data may include but is not limited to additional and historical information on accountability, assessment, learning environment, program review, student health, kindergarten readiness and school finance.

Chapter 3. Data Use

Kentucky public school education and other data are appropriately used by teachers, administrators and policymakers at classroom, school, district and national level to empower educators, students and families with the information they need to make decisions to help all learners succeed. Data is used for public, state and federal reporting, state funding calculations, administering state assessments, school accountability, early childhood school readiness and to improve programs and inform instruction. In instances where using personal information is necessary, those few individuals who have access to this information to carry out their duties must handle it in a legal, responsible and ethical manner.

LEA Data Use

Teachers use data to understand how their students are learning, to help each student be successful and to make changes in instruction. Schools use data to support continuous improvement and teacher effectiveness. Districts use the data they collect from schools to make decisions on resources, such as facilities and transportation that each school needs to support its students.

KDE Data Use

KDE uses data to conduct ongoing program evaluation and research, measure how districts are meeting goals for students, provide tools back to districts to inform instruction, assess how state funds are improving education, fulfill state and federal reporting requirements, and provide aggregate information to the public.

KDE staff who have been granted access to personal or confidential data must use the data only for the purpose for which access was granted and only in the performance of their assigned duties and tasks. In addition, they will take steps to ensure the ongoing protection and privacy of such data, including appropriate disposal and protection from disclosure to unauthorized individuals.

Federal Data Use

The United States Department of Education (USDOE) uses data provided by states for policy development, planning and management, and monitoring of individual states' federally funded programs under the Elementary and Secondary Education Act (ESEA) (appendix O). KDE does not provide the USDOE access to any of the personally identifiable information in KDE's data systems. All data elements collected and transferred to the USDOE are based on the reporting requirements contained in EdFacts (appendix O), USDOE's prescribed approach for states to comply with reporting requirements for program monitoring and performance reports under 34 CFR 76.720. KDE reported data to EdFacts includes only aggregated data with no personally identifiable data.

External Data Use

KDE may disclose PII from an education record of a student if the disclosure meets either the "Studies or Audit or Evaluation" exception outlined in *20 U.S.C. § 1232g(b) and (h) – (j) and 34 CFR § 99.31 (appendix O).*

Studies

KDE may disclose confidential, personally identifiable information of students to entities in order to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction. Disclosure is authorized under the FERPA Studies Exception. The KDE shall enter into an MOU prior to releasing data (appendix K).

Audit/Evaluation

KDE may disclose confidential, personally identifiable information of students to entities to audit or evaluate a federal- or state-supported education program; or enforce or comply with federal legal requirements related to the program. The receiving entity must be a state or local authority or other FERPA-permitted entity or must be an authorized representative of state or local educational authority or other FERPA-permitted entity. Disclosure is authorized under the FERPA Audit-Evaluation Exception. The KDE shall enter into an MOU prior to releasing data (appendix L).

Under either FERPA exception, disclosure shall be made only if (1) the conditions in FERPA regulation *34 CFR 99.31(a)* are met and (2) the request for data sharing must be approved by KDE with a fully executed KDE Memorandum of Understanding (MOU). The MOU includes specifics on how the information will be protected to shield personal identification of students by others and how the information will be destroyed when no longer needed.

External data requests must: (1) meet the FERPA exception requirements, (2) align to agency strategic initiatives, and (3) have the support of a KDE associate commissioner.

The KDE uses a multi-step process, facilitated primarily by the Chief Data Officer and the Data Governance Committee, which includes staff from all KDE offices including the Office of the Commissioner. To begin the process, external requesters must complete a Data Request Form (appendix F). If the Committee approves the request, the requesting entity must complete the approved KDE Memorandum of Understanding (MOU) template.

The MOU is a legally binding document that authorizes the researcher, as an agent of KDE, to carry out evaluations, audits, or compliance activities or conduct research for or on behalf of KDE. The MOU details the researcher's/authorized agent's responsibilities with respect to protecting the privacy of the students or staff whose information will be provided for the study or audit/evaluation and includes a nondisclosure affidavit that must be signed by each individual who will have access to the data provided. All MOUs executed or amended on or after January 1, 2015 with whom the KDE discloses "personal information" shall include provisions of Kentucky's Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931, 61.932 and 61.933 (appendix O). Those provisions include utilization of security and breach investigation procedures that are appropriate to the nature of the personal information disclosed; notifying KDE of a security breach relating to personal information within seventy-two hours of discovery of an actual or suspected breach; and cooperating with KDE in complying with the response, mitigation, correction, investigation, and notification requirements of the Act.

Researchers must comply with all applicable laws and regulations (appendix O) as well as applicable portions of this policy (KDE's Data Collection, Access and Use Policy). KDE will not release data until the MOU has been fully executed. As part of the agreement, researchers are required to provide a copy of products resulting from the research (e.g., publication, report, book) to the KDE Chief Data Officer and to verify destruction of the data once the research is completed.

Record of Disclosure

In compliance with FERPA guidelines, KDE maintains a record of all disclosures of PII from education records to organizations made under FERPA exceptions.

Retention

For guidance on retention, refer to the State Government Records Retention Schedules and the KDE-specific schedule (appendix M).

Destruction of Data

Information that has met the retention schedule must be removed, destroyed or deleted in an appropriate manner (appendix D-9).

KDE requires any party receiving personally identifiable information to permanently destroy such information when it is no longer needed for the purpose specified in the terms of the signed MOU using an application that will permanently destroy the data. The party must describe the application and methods that will be used to destroy all confidential data in their MOU, Exhibit D. The entity must confirm, in writing, that the confidential data was destroyed, the method(s) used and the date of the destruction.

Appendices

A. Acronym Reference Guide

B. Definitions

C. Data Controllers/Data Governance Committee

D. Data Guidelines and Procedures

1. Data Breach
2. Data Collection Request Form (KDE use only)
3. Enterprise Data Dictionary
4. Data Collection Calendar (available soon)
5. Data Standards
6. Data Security Training Plan (available soon)
7. Data Security Video Series
    a. What is PII?
    b. Data Access and Sharing
    c. Was that a Data Breach
8. External Data Use
9. Destruction of Data
10. System Access Control (4/4/2016)

E. Data Governance Organizational Chart

F. Data Requests

G. Data Request Form

H. Data Stewards

I. Employee Affidavit of Nondisclosure

J. FERPA Exceptions Summary

K. MOU – Studies

L. MOU – Audit/Evaluation

M. State Government Records Retention Schedules

N. Data Policies

1. Data Governance
2. Data Collection, Access and Use
3. Data Security Policy - Work in Process

O. Summary of key state and federal laws regarding education and other personal information

P. United States Department of Education (USDOE) Ed facts

Q. Other Resources and Best Practices

1. Privacy Technical Assistance Center (PTAC)
2. Data Quality Campaign
3. National Forum on Education Statistics

R. Data Definitions

A fundamental piece of any data quality infrastructure is a standardized set of precise data definitions. The following definitions are derived from KDE policies, implementation guidelines and other related documents.

Authoritative Source: the recognized or official data production source for a data asset that is identified as reliable and accurate. If two or more systems have mismatched information, the authoritative data source is used as the most correct.
Data Definition: In some cases, the U.S. Department of Education (through the National Center for Education Statistics), the U.S. Office of Management and Budget, or the No Child Left Behind Act maintains a definition of a required data element. Where federal definitions do not exist, a standard definition should be used for all districts and schools in the state. It is important that the definition be adopted uniformly across all data systems.
Data Element*:* the fundamental data structure in a data processing system. Any unit of data defined for processing is a data element; for example, ACCOUNT NUMBER, NAME, ADDRESS and CITY. A data element is defined by size (in characters) and type (alphanumeric, numeric only, true/false, date, etc.). A specific set of values or range of values may also be part of the definition.
Data field: the physical unit of storage in a record. For example, the data element SSID, which exists only once, is stored in the SSID field in each student record and in the SSID field in each order record.
Data Governance Processes: processes established by the Data Governance Committee, including but not limited to, the steps to be followed for data policy development, roles and responsibilities for data governance, and change management of KDE data.
Data Standard: Data Standards are documented agreements on representation, format, definition, structuring, tagging, transmission, manipulation, use, and management of data.
Data*:* any form of information whether on paper or in electronic form. Data may refer to any electronic file no matter what the format: database data, text, images, audio and video.
De-Identification of Data: the process of removing or obscuring any personally identifiable information from student records in a way that minimizes the risk of unintended disclosure of the identity of individuals and information about them.
Directory Information: defined by FERPA is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Typically, “directory information” includes information such as name, address, telephone listing, participation in officially recognized activities and sports, and dates of attendance. A school may

disclose “directory information” to third parties without consent if it has given public notice of the types of information which it has designated as “directory information,” the parent’s/guardian’s or eligible student’s right to restrict the disclosure of such information, and the period of time within which a parent/guardian or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as “directory information.” The means of notification could include publication in various sources, including a newsletter, in a local newspaper, or in the student handbook. The school could also include the “directory information” notification as part of the general notification of rights under FERPA. The school does not have to notify a parent/guardian or eligible student individually. (34 CFR § 99.37.) Directory information does not include a student’s: (1) Social security number; or (2) Student identification (ID) number, except when a student ID number, user ID, or other unique personal identifier is used by the student for purposes of accessing or communicating in electronic systems, but only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user’s identity, such as a personal identification number (PIN), password, or other factor known or possessed only by the authorized user.
Disclosure: to permit access to, release, transfer, or otherwise communicate personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means.
Enterprise Data Dictionary: a centralized descriptive list of names (also called representations or displays), definitions and attributes of data elements to be collected in an information system or database, designed to standardize definitions and ensure consistency of use by the enterprise.
Enterprise: P-12 school districts, higher education, other state agencies and vendors and/or partners.
Family Educational Rights and Privacy Act (FERPA): a federal law that affords parents/guardians the right to have access to their children’s education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old, or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents/guardians to the student (“eligible student”). The FERPA statute is found at 20 U.S.C. 1232g and the FERPA regulations are found at 34 CFR Part 99.
Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of health information needed for patient care and other important purposes.
Individuals with Disabilities Education Act (IDEA) is a law ensuring services to children with disabilities throughout the nation. IDEA governs how states and public agencies provide early intervention,

special education and related services to more than 6.5 million eligible infants, toddlers, children and youth with disabilities.
KDE Data Governance: KDE offices, employees, policies, processes and technology creating a consistent view of KDE data; includes roles and responsibilities, committees and committee charters that collectively describe how decisions are made, monitored and enforced regarding the management of KDE data.
Local Education Agency (LEA): a collective term used to include public elementary, secondary and technical schools, districts or other administrative agencies for schools or state postsecondary institutions or organizations.
National School Lunch Act (NSLA): established a federally assisted meal program operating in public and nonprofit private schools and residential childcare institutions. It provides nutritionally balanced, low-cost or free lunches to children each school day.
Open House: the network of systems that collect, store and report data to support the operations and objectives of KDE.
Personally identifiable information (PII): includes, but is not limited to: the student's name; the name of the student's parent/guardian or other family member; the address of the student or student's family; a personal identifier, such as the state student identifier; personal characteristics or other information that would make the student's identity easily traceable. A small set of this information is used for assigning identifiers and for identifying students who have transferred from another district within the state or who have returned to the state who already have identifiers.
Privacy: an individual's right to freedom from intrusion due to disclosure of information without his or her consent.
Privacy Technical Assistance Center (PTAC): a branch of the U.S. Department of Education that offers technical assistance to State educational agencies, local educational agencies, and institutions of higher education related to the privacy, security, and confidentiality of student records. PTAC was created to respond to the need for clarification for states and other education stakeholders on policy, technical/data security, and legal issues about student privacy. For additional information, FAQs, and other resources, please visit PTAC's website: *http://ptac.ed.gov*.
Protection of Pupil Rights Amendment (PPRA): (20 U.S.C. § 1232h; 34 CFR Part 98) applies to programs that receive funding from the U.S. Department of Education (ED). PPRA is intended to protect the rights of parents/guardians and students in two ways: It seeks to ensure that schools and contractors make instructional materials available for inspection by parents/guardians if those materials will be used in connection with an EDfunded survey, analysis, or evaluation in which their children participate; and It seeks to ensure that schools and contractors obtain written parental

consent before minor students are required to participate in any ED-funded survey, analysis, or evaluation that reveals information concerning: 1) Political affiliations; Mental and psychological problems potentially embarrassing to the student and his/her family; Sex behavior and attitudes; Illegal, anti-social, self-incriminating and demeaning behavior; Critical appraisals of other individuals with whom respondents have close family relationships; Legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers; or Income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).
Statewide Student Identifier (SSID): a unique, non-personally-identifiable number linked to a given individual student within the Kentucky public P–12 educational system. SSIDs are used to maintain data on individual students, such as linking students to statewide assessment scores and tracking students in and out of schools and LEAs in order to determine more accurate dropout and graduation rates.
Suppression: a disclosure limitation method which involves removing data (e.g., from a cell or a row in a table) to prevent the identification of individuals in small groups or those with unique characteristics. This method may often result in very little data being produced for small populations, and it usually requires additional suppression of non-sensitive data to ensure adequate protection of PII (e.g., complementary suppression of one or more non-sensitive cells in a table so that the values of the suppressed cells may not be calculated by subtracting the reported values from the row and column totals). Correct application of this technique generally ensures low risk of disclosure; however, it can be difficult to perform properly because of the necessary calculations (especially for large multi-dimensional tables). Further, if additional data are available elsewhere (e.g., total student counts are reported), the suppressed data may be re-calculated.