# Kentucky Department of Education

Policy Type: Data

Title: Data Collection, Access, and Use Policy

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

## Revision 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 |
| 2.1 | 03/11/2019 | Linda Burton | Updates to conform to current organizational structure, provide 508 Accessibility compliance |
| 2.2 | 10/12/2022 | Data Governance Committee | Updated per Data Governance Committee edits. |
| 2.3 | 9/11/2024 | Data Governance Committee | Updates and clarifying language added especially to identify responsibilities for data sharing with vendors and non-student data. Approved by DG and OLS/Swartz. |

| Approval | Date |
|---|---|
| 2.0 - Core Process Team – Review | 8/27/2015 |
| 2.0 - Chief Information Officer/KIDS Associate Commissioner - Approval | 9/10/2015 |
| 2.1 - Data Governance Committee – Review | 3/11/2019 |
| 2.1 - Core Process Team/Chief Information Officer – Technical updates; Review not required | N/A |
| 2.2 – Technology Planning Council/Chief Information Officer – Approved | 3/28/2023 |
| 2.3 – Technology Planning Council/Chief Information Officer – Approved | 11/04/2024 |

## Authority

The Data Governance Committee will review the *Data Collection, Access, and Use Policy* annually or as needed; when there is a change to a data collection, access or use activity; and upon request by the KDE Technology Planning Council. If, at any time, a portion of this policy conflicts with any 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 (KDE Data Governance Policy). The committee operates under the authority of the KDE chief information officer (CIO) and the Technology Planning Council. The CIO and Technology Planning Council review and make determinations on the 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 by email to KDE Data Services, (kdedataservices@education.ky.gov) or by telephone at (502) 564-2020.

## Purpose and Scope

The Kentucky Department of Education (KDE) is responsible for the 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; the Kentucky Family Educational Rights and Privacy Act, KRS 160.700 et seq.; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g and 34 CFR Part 99; the Richard B. Russell National School Lunch Act, 42 U.S.C. 1751 et seq., the Child Nutrition Act of 1966, 42.U.S.C. 1771 et seq., and 7 CFR 245.6; the Personal Information Security and Breach Investigation Procedures and Practices Act, KRS 61.931 et seq.; the Individuals with Disabilities Education Act (IDEA), 20 U.S.C. 1400 et seq., 34 CFR Part 300 and 34 CFR Part 303; the Children's Online Privacy Protection Act, 15 U.S.C. 6501 et seq. and 16 CFR Part 312; and the Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. § 1232h and 34 CFR Part 98. 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 the *KDE 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

# Data Collection

Schools collect information including, but not limited to, grades, program participation, demographics, attendance, and health/immunization data. It should be noted that a student's health records, including immunization records, maintained by an educational agency generally constitute education records subject to FERPA and are not covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (See 45 CFR § 160.103). 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, education programs, 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 decision-making, reporting, audits, and evaluation. The Systems Catalog (accessible to KDE staff) provides information about Kentucky's statewide information systems.

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

At the time a student is first enrolled into a Kentucky public PK–12 educational program, the Infinite Campus student information system assigns each student a statewide student identifier (SSID), which is a unique, non-personally identifiable number. 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 to determine more accurate dropout and graduation rates.

The first time a staff record is created in the student information system, the system assigns each LEA staff a Person ID or Employee Number, which is a locally unique, non-personally identifiable number. 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.

Kentucky identifies educators through the assignment of Education Professional Standards Board (EPSB) identification (EPSB ID) numbers. An EPSB ID number is assigned when a prospective individual creates an account in the Kentucky Educator Credentialing System (KECS). The EPSB ID number will remain unchanged as a person moves between schools, districts, or out-of-state and returns to teach. To ensure data accuracy, it is imperative that each school and district include the EPSB ID number in all district and school management systems. All individuals who create a KECS account will be assigned an EPSB ID, including KDE staff, postsecondary staff involved with the certification of their students, and district/school staff who are involved in an educator's hiring.

## Authoritative Source

The Data Governance Committee determines the authoritative source system for each data asset. 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 and Change Request Form. The Data Governance Committee will review the request to evaluate its impact on KDE and LEAs and, when applicable, will provide LEAs with an opportunity for input.

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

## Quality Control

Data stewards are responsible for the management and oversight of KDE's enterprise data assets to provide high-quality data that is easily accessible in a consistent manner. See the KDE Data Governance Policy 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 collection and data use. The KDE Enterprise Data Dictionary (available on the Common Education Data Standards site) identifies and describes federally reported 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 the 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 and regulations 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 indicates. 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.

# 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. See Appendix O for a summary of key state and federal statutes and regulations that provide specific protections 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 personally identifiable and confidential data based on job and role-specific needs that correspond to a specific educational “need to know” purpose.

For access to enterprise systems, KDE requires staff upon employment to sign appropriate access agreements including, but not limited to, the KDE Employee or Contractor General Affidavit of Nondisclosure (Appendix I).

KDE staff who have a job-related 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 approve staff person 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 email address require approval and signature of the KDE chief information officer. Access to all other person-level data requires approval from the relevant office’s associate commissioner or data controller. 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., access his/her own child’s records and research for a dissertation). Employees must maintain the privacy and security of all confidential or personally identifiable records.

Supervisors must ensure that staff who are changing their job duties within KDE shall have their access and operational privileges reviewed immediately and when 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 to perform 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.

The KDE Data Governance SharePoint site is available to KDE staff and includes training materials and other resources supervisors should use for new staff orientation. Other training will be made available to address topics according to the agency training plan.

## Parent/Student Access

Parents and students are provided access to their education records through the Infinite Campus Parent or Student portal and associated mobile application. Any request for additional access to records maintained by a school or district should be made to the applicable school or district.

## 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 website. For information about Open Records Requests to KDE, Kentucky Board of Education, and Education Professional Standards Board, visit KDE's website at Open Records Requests - Kentucky Department of Education.

## 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

KDE may on a case-by-case basis 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 work with the district of enrollment to record in the student’s education records the articulable and significant threat to the health or safety of a student or other individuals that formed the basis for disclosure and the parties to whom the information was disclosed (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 on the Kentucky School Report Card Suite and Open House 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 gender) or micro data (such as individual-level student assessment results by grade and school). It is important to note that PII is not limited to only direct identifiers, such as names, student IDs or social security numbers, but also includes 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 U.S. Department of Education Privacy Technical Assistance Center and the Family Policy Compliance Office guidelines and best practices in regard 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 Suite

KDE publishes School Report Card information specific to each school and district that includes test performance, teacher qualifications, student safety, parent involvement and much more. The school and district report cards were established by statute and regulation (KRS 158.6453 and 703 KAR 5:140). Additionally, the report cards incorporate the requirements of the federal Every Student Succeeds Act (ESSA).

## School Report Card Suite Supplemental Data

KDE publishes Supplemental Data after publication of the annual School Report Card Suite. 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.

# 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 provide educators, students and families with the information they need to make data-driven 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 guide changes in instruction. Schools use data to support continuous improvement and teacher effectiveness. Districts use data they collect from schools to make decisions on resources, such as facilities and transportation that each school needs to support its students.

## KDE Internal Data Use

KDE uses data to conduct ongoing internal program evaluation and research, measure how districts are meeting goals for students, provide tools for 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. For sharing data outside of KDE, refer below to External Data Use.

## Federal Data Use

The United States Department of Education (USDOE) uses data provided by states for policy development, planning, management and monitoring of individual states' federally funded programs under the Every Student Succeeds Act. KDE collects and reports data to USDOE based on federal reporting requirements, including EDFacts and USDOE's prescribed approach for compliance with reporting requirements for program monitoring and performance reports under 34 CFR 76.720.

## External Data Use

The KDE uses a multi-step review and determination process for requests to disclose data to external entities. The process is primarily facilitated by the chief data officer and the Data Governance Committee which includes staff from all KDE offices including the Office of the Commissioner.

Any external data requests must: (1) be allowable under applicable law, (2) align to KDE's strategic initiatives, and (3) have the support of a KDE associate commissioner.

A memorandum of understanding (MOU) must be executed for requests utilizing the FERPA studies (34 CFR 99.31(a)(6)) or audit or evaluation (34 CFR 99.31(a)(3) and 99.35) exceptions.

Studies (34 CFR 99.31(a)(6)) – KDE may disclose confidential, personally identifiable information of students if "[t]he disclosure is to organizations conducting studies for, or on behalf of, educational agencies or institutions to: (A) Develop, validate, or administer predictive tests; (B) Administer student aid programs; or (C) Improve instruction." The KDE shall enter into an MOU prior to releasing data under the FERPA studies exception (appendix K).

Audit or Evaluation (34 CFR 99.31(a)(3) and 99.35) – 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 KDE shall enter into an MOU prior to releasing data under the FERPA audit or evaluation exception (appendix L).

Other Non-Student Data – KDE may disclose personally identifiable information or other confidential non-student data to an approved data recipient upon written request under the general terms of a fully executed KDE Confidential Data MOU. Non-student personally identifiable information is identified similar to FERPA's definition of PII for students and includes information that would make a non-student identity easily recognized (by itself or in combination with other factors).

External requesters must complete a Data Request Form (appendix F). The Data Governance Committee reviews the request and makes a determination to approve or reject the request. If the data request meets all criteria and is approved, the requesting entity must complete the approved KDE Memorandum of Understanding (MOU) template. KDE approved data sharing templates are available to download on the KDE Data Requests webpage.

## Record of Disclosure

The KDE Data Request process creates a record of data requests and disclosures of PII from education records.

## 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-8).

KDE requires any party receiving personally identifiable information to permanently and irrevocably destroy such information when it is no longer needed as specified in the terms of the signed MOU. 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. Data Definitions

C. Data Controllers/Data Governance Committee

D. Data Guidelines and Procedures

  1. Data Breach
  *2.* Data Collection and Change Request Form
  3. Enterprise Data Dictionary
  4. KDE State Report Submissions
  5. Data Standards
  6. Data Privacy and Security laws, best practices and resources
  7. External Data Use
  8. Destruction of Data

E. Data Governance Organizational Chart

F. Data Requests

G. Data Request Form

H. Employee Affidavit of Nondisclosure

I. FERPA Exceptions Summary

J. MOU - Studies

K. MOU – Audit/Evaluation

L. MOU – Confidential Data

M. State Government Records Retention Schedules

N. Data Policies

  9. Data Governance
  10. Data Collection, Access and Use

O. Summary of key state and federal laws regarding confidentiality, privacy and security of education and other personal information

P. United States Department of Education (USDOE) EdFacts

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 Every Student Succeeds 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 the 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 that 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, 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 to permit 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.

**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 and already have identifiers.

**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: https://studentprivacy.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 ED funded 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 or beliefs of the student or the student's parents; Mental or psychological problems  of the student or the student's family; Sex behavior or attitudes; Illegal, anti-social, self-incriminating or 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; religious practices, affiliations, or beliefs of the student or student's parent; and 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 to determine more accurate dropout and graduation rates.

**Suppression**: a disclosure limitation method that 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 a 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.