KENTUCKY DEPARTMENT OF EDUCATION DATA GOVERNANCE POLICY

Policy type: Data

Title: Kentucky Department of Education (KDE) Data Governance

Effective Date: March 1, 2009

Responsible Party for Policy Implementation: Commissioner

Applicability (personnel complying with policy): KDE Agency, Contractors and Vendors

Background

Revision History

Version	Date of Issue/Update	Author(s)	Brief Description of Revision
1.0	1/21/09	Data Policy Committee	Original policy
1.1	2/2/09	Data Policy Committee	Definition revisions
1.2	1/29/10	Data Policy Committee	Data Policy Program Coordinator language
1.3	1/28/11	Data Policy Committee	Updated to reflect new governance structure
1.4	4/6/2015	Data Governance Committee	Updated to include selected Data Policy Committee Charter information and streamlined data governance structure
1.5	3/26/2018	Data Governance Committee	Updates to conform to current organizational structure and provide 508 Accessibility compliance, added Data Governance committee determination for disclosures to third parties and Data Steward responsibility
1.6	3/11/2019	Data Governance Committee	Technical updates Only
1.7	12/7/2022	Data Governance Committee	Added chief data privacy officer role and edits for clarity.

Reviewed by/Approving authority	Date
1.4 - KDE Technology Planning Council - Review	4/23/2015
1.4 - Chief Information Officer/Office of Education Technology (OET) Associate Commissioner - Approval	4/23/2015
1.5 – KDE Technology Planning Council – Review	3/31/2018
1.6 – Data Governance Committee – Approval	3/11/2019
1.7 – KDE Technology Planning Council/Chief Information Officer – Approved	3/28/2023

If you have questions about this document, contact KDE's chief data officer at (502) 564-2020.

Contents

Authority

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. The rest of the policy shall remain in effect.

The Data Governance Committee operates under the authority of the KDE Technology Planning Council (TPC) and KDE Chief Information Officer (CIO). The CIO and Technology Planning Council mandate data governance policies approved by the Data Governance Committee.

Purpose and Scope

The Data Governance Policy further defines, based on the Kentucky Education Technology System (KETS) Master Plan, the KDE's structure for data governance including critical roles, decision-making authority, responsibilities and associated activities, and accountability of individuals and groups that encounter enterprise data assets.

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 shall support, participate and promote KDE's data governance policies and processes.

Vision

Our vision is to ensure stakeholders have access to timely, consistent and accurate data resulting in quality data-driven decisions affecting student learning. The KDE recognizes that decisions are only as good as the data on which they are based. To transform data into information to facilitate wise decision-making, enterprise systems users and managers of K-12 data need a clear understanding of data definitions, data and process ownership and authority, accountability, security, and reporting needs and requirements, as well as the processes and timelines around each. This policy involves stakeholders throughout KDE to address those needs. Data collected, stored, processed and disseminated by the KDE are agency resources and must be managed from an enterprise perspective.

Mission

Our mission is to improve data accuracy, usability, timeliness and security while meeting the needs of all education stakeholders.

Guiding Principles

1. Ensure that proper data use and management are integral in KDE's administration of everyday services.
2. Establish clear high-level, agency-wide sponsorship of data governance and integrate accountability for successful data management throughout all levels of the agency.

3. Establish data stewards and data controllers by identifying those people/positions within each program or office who are accountable for the creation, definition, security and integrity of data assets and have day-to-day responsibility for program data collection and use. It is essential that these individuals be respected, influential and subject matter experts within the organization.
4. Incorporate data steward activities into the regular, day-to-day aspects of data stewards' and data controllers' jobs. In most cases, data steward is not a job-title or a new position; data stewardship is one of the responsibilities of a person's position.
5. Establish protocols that respect a distinction between the ability to collect and/or provide data and the authority to collect and/or provide data. "Can we? Should we?"
6. Promote a culture of data quality that includes inspection and validation of key data elements.
7. Establish agency policies for high-level data matters and provide guidelines to support consistent implementation.
8. Establish data access protocols that establish and verify the need for access to data sets while protecting confidentiality and security of data. Data access protocols will outline needed authorization of data use.
9. Establish data disclosure protocols that guide appropriate and allowable disclosure of data from education records to third parties, such as researchers, contractors and others.
10. Invest the necessary agency support to make data governance efforts successful.

KDE Data Governance Structure

Key Roles

The Technology Planning Council, chief information officer and chief data officer have responsibility for day-to-day operational management and decision making for the agency's enterprise data.

Data Governance Committee members and alternates will be appointed by each associate commissioner and shall serve indefinitely. If a member terminates from the committee, the respective associate commissioner shall appoint, within a reasonable amount of time, a replacement. The Data Governance Committee provides input to the chief data officer and chief information security officer.

The chart below illustrates the composition of key roles and groups that share responsibility for KDE's data governance.

Key Roles and Groups	Composition
KDE Technology Planning Council	Agency leadership including Office of Education Technology (OET) associate commissioner/chief information officer, associate commissioners (or designees) and district CIO representatives
Chief Information Officer (CIO)	OET associate commissioner
Chief Data Officer (CDO)	School Data Services Division director
Chief Data Privacy Officer (CDPO)	KDE data privacy subject matter expert
Chief Information Security Officer (CISO)	KDE Information Security Program manager
Data Governance Committee	One or more data controller representatives from each KDE office
Data Steward	Expert on an assigned data asset
Data Controller	Lead data point of contact for each office and member of Data Governance Committee

Responsibilities by Role

Associate Commissioner: provides resources for implementation of approved policies. An associate commissioner has senior-level authority for all aspects of data activities for his/her respective office and program areas, and has primary responsibility to provide a management commitment and vested interest in the decisions affecting enterprise data.

Chief Data Officer (CDO): primary KDE point person for data availability, reporting, and data quality initiatives. CDO chairs the Data Governance Committee. The CDO manages or coordinates data initiatives with partner agencies and the vendors used in completing enterprise data activities. The CDO escalates unresolved data issues to the CIO and Technology Planning Council. The CDO coordinates a cross-office relationship among data governance adherents. The CDO monitors the development and maintenance of the KDE Enterprise Data

Dictionary (available in the [Common Education Data Standards site](#)), data collections and data reporting events.

Chief Data Privacy Officer (CDPO): primary KDE point person whose role is to protect the privacy of data across the agency whether the data is generated by or collected for students and individuals. The CDPO is responsible for accounting and inventory of all data the organization receives, allowed use of the data, and oversees processes and procedures governing privacy controls for data received and collected.

Chief Information Officer (CIO): senior executive responsible for KDE information technology and systems supporting enterprise goals. The CIO has decision-making authority for enterprise data matters and oversight in the development and implementation of policies.

Chief Information Security Officer (CISO): primary KDE point person responsible for security of information in both physical and digital form, and for accounting and inventory of all data the organization receives. The CISO is responsible for the overall security stance of the department, which includes the data systems.

Data Controller: an individual assigned to serve as lead data steward/controller for a KDE Office. It is essential that a data controller be respected, influential and a subject matter expert. Each data controller reports directly to the associate commissioner of their office and represents his/her KDE office as member of the Data Governance Committee. In conjunction with his/her respective associate commissioner, the data controller ensures that office personnel are trained on KDE data governance policies and implementation guidelines, FERPA requirements, data ethics, data security and best practices, and respective office personnel perform their duties accordingly. Each data controller is responsible for ensuring that data assets under the jurisdiction of his/her respective office are assigned to a data steward.

Data Controller Alternate (Backup): an individual assigned to serve as alternate (backup) for his/her respective office's data controller. It is essential that the alternate is qualified and prepared to assume the duties of the data controller at any time. In the absence of the data controller, the alternate will represent the office as a member of the Data Governance Committee.

Data Governance Committee: oversees data projects and data quality initiatives, systematically creates and maintains enterprise data policies, an agency-wide training plan and communication plan, and defines the roles, responsibilities, and guidelines for collecting, using and reporting data. This includes, but is not limited to, the adoption of common definitions, standards, processes, practices, implementation guidelines and products. The Data Governance Committee resolves data governance issues affecting agency data. The Data Governance Committee makes determinations to approve or deny proposed or requested changes for an enterprise system, changes, additions, or removal of a data asset, and disclosures to third parties of personally identifiable data. In the event the Data Governance Committee does not reach agreement on an issue, the data controller responsible for the data asset will present the proposal or request to the Technology Planning Council.

Data Steward: an individual assigned responsibility for a data asset, which can be a data element, data field or data collection. The data steward should be the expert on the assigned data asset and is responsible for hands-

on work within KDE related to the assigned data asset. The data steward will serve as the operations point of contact for the data asset's references and metadata contained in the KDE Enterprise Data Dictionary. A data steward has day-to-day responsibilities including:

- maintain an up-to-date data definition and/or formula,
- identify the data collection frequency and date(s),
- analyze the impact of state and federal laws and regulations, and policies on the collection and reporting of assigned data asset,
- provide recommendations on required/target level of accuracy and inspect data to ensure it meets the established level of accuracy,
- document reporting requirements and date(s),
- maintain an up-to-date data standard for the assigned data, provide requirements to develop, document and maintain state reports, ad hoc reports and custom reports for validation,
- communicate with and support district and KDE staff on the appropriate/allowable use of the data,
- inspect the data for quality, completion and validation in accordance with specified collection periods and at end of year,
- initiate appropriate actions to improve or resolve identified data quality issues,
- respond to questions concerning the data asset and to inquiries on appropriate/allowable data use,
- promote data use for data driven decision making, and
- adhere to FERPA requirements and best practices for data ethics and data security.

School Data Services Division: champions sharing of information and systems that support data sharing. The team promotes availability, sharing and maximizing the quality and use of agency data. The team is responsible for management of the KDE Data Dictionary and master reporting schedule. Team members serve as liaisons with data stewards to help resolve systematic data quality issues that cross all agency and district data systems.

Technology Planning Council: reviews and contributes to data policies and resolves issues when the Data Governance Committee cannot reach consensus or when consulted by CIO. The council provides oversight of information technology (IT) and data strategic planning, application portfolio management, project review, prioritization and approval.

Appendices

Acronym Reference **(Internal Document)**

Definitions **(Section R, Pages 12-15)**

Data Request Form

KDE Information Technology Organizational Chart **(Internal Document)**

Kentucky K-12 Data Quality Study

MOU – Studies Template

MOU – Audit/Evaluation Template

KDE Data Controllers/Data Governance Committee

KDE Data Stewards

KDE Employee Affidavit of Nondisclosure **(Internal Document)**

Related KDE Policy

Data Collection, Access and Use Policy