

KENTUCKY DEPARTMENT OF EDUCATION

STAFF NOTE

Review Item:

702 KAR 1:170, School District Data Security and Breach Procedures (Second Reading)

Applicable Statute or Regulation:

KRS 61.931

KRS 61.932

KRS 61.933

KRS 365.734

200 KAR 1:015, Data Breach Notification Forms

Action Question:

Should the Kentucky Board of Education approve 702 KAR 1:170?

History/Background:

Existing Policy. In 2006, the Kentucky General Assembly passed House Bill 341, which mandated the Kentucky Department of Education (KDE) to conduct a study of the requirements for data security and a notification process when a data breach occurs. The resulting House Bill 341 data security study provided this information and has remained an effective cornerstone of guidance for both Kentucky's school districts and for the Kentucky Department of Education. In the intervening years, the Kentucky Department of Education has, at least annually but usually more often, reminded districts of the importance of data security, breach prevention, and notification via webcast or face-to-face meetings.

On January 1, 2015, a new state law, the Personal Information Security and Breach Investigation Procedures and Practices Act (KRS 61.931, .932, .933, and .934) went into effect. This legislation, more commonly known as "House Bill 5," focuses on notification of victims of data theft or misuse, and protection of personally identifiable information (PII). It applies to every state agency, including KDE, every public school district, and every vendor holding a contract with a state agency or school district.

Also in effect since January 1, 2015, is a new chapter in KRS 365 designed to protect student data from misuse by cloud service providers. Formerly known as House Bill 232, this legislation defines "student data" and limits its use to educational purposes, unless otherwise agreed to in writing by the students' parents or as permitted by the Family Rights and Privacy Act (FERPA).

Both pieces of legislation authorize the Kentucky Department of Education to promulgate administrative regulations for the purpose of providing guidance to public school districts.

The proposed administrative regulation will require KDE and each district to, at least annually, review best practices for prevention of data breaches, preparation of notification, and finally, notification to victims of a data breach. Each district will need to weigh its own risk against the costs, which can be significant, of implementing each best practice. Because of this, there may be significant differences in the approach each district believes is best and affordable to take. Second, the proposed regulation will require districts and KDE to communicate to their respective boards prior to August 31 of each year, which best practices they are taking, or not taking, based upon their own evaluation of risk and available budget.

The Kentucky Department of Education has developed the [Data Security and Breach Notification Best Practice Guide](#), which provides recommendations to districts and to KDE on data protection, loss prevention and notification as well as summarizing requirements on what to do in the event of a data breach. It appears on the board's online materials site.

There are two significant revisions since the first reading of the regulation at the June 2015 meeting of the Kentucky Board of Education:

1. The Data Security and Breach Notification Best Practice Guide mentioned above will now be incorporated by reference in the regulation and this will require that we bring it back to the Kentucky Board of Education when the document requires updating in order to incorporate any needed updates or revisions.
2. Section 5 has been added to the regulation. This section includes new language providing specific direction to districts on the procedure for their breach notification to KDE. This language maintains that the Best Practice Guide as a whole is still optional for a district, but provides specific direction and clarification on the breach notification procedure.

Impact on Getting to Proficiency:

Approval of this regulation will ensure that there is an appropriate and consistent emphasis on data security at the school and district levels as well as the Kentucky Department of Education. The incorporated documentation will provide best practices and guidelines for the reasonable security and breach investigation procedures and practices to be utilized. This may not result in an immediate or direct impact on student achievement; however, it does put into effect safeguards to secure the data and provide a safe learning environment where student achievement can then become the primary focus.

Groups Consulted and Brief Summary of Responses:

The approach and wording for 702 KAR 1:170 was discussed and reviewed extensively through both onsite/in-person and web conferencing opportunities. All groups/individuals listed below are in support of the proposed regulation for School District Data Security and Breach Procedures.

- District education technology leadership (Chief Information Officers, District Technology Coordinators, Chief Education Technology Officers)
- District Superintendents

- KDE Executive Leadership
- KDE Data Governance Committee
- KDE Core Process Team
- Local Superintendents Advisory Council

The input from these groups will be discussed at the August KBE meeting.

Contact Person:

David Couch, Associate Commissioner
Office of Knowledge, Information and Data Services (KIDS)
(502) 564-2020, ext. 2229
David.Couch@education.ky.gov



Commissioner of Education

Date:

August 2015