Spencer County Schools
Data Security and Privacy
2023 - 2024

Purpose

Basic awareness of data security and privacy best practices. Notification to the Spencer County School Board that the district has reviewed and is implementing best practices.

Current and Relevant Legislation

Federal

FERPA (1974) - Family Rights and Privacy Act
COPPA (1998) - Children's Online Privacy Protection Act
CIPA (2000) - Children's Internet Protection Act

State

Kentucky FERPA (1994)
KRS 160.700 et seq (See Appendix A)
The Family Education Rights and Privacy Act limits disclosure of personally identifiable data except under certain conditions. KDE limits access to identifiable data but does promote use of aggregated data for analysis and research. Public data is available through the Open House site.

FERPA gives parents certain rights with respect to their children's education records. A school must provide a parent with an opportunity to inspect and review his or her child's education records within 45 days following its receipt of a request.

House Bill 232 (2014)
Called for creation of KRS 365.734 (See Appendix A)
Prohibits certain uses of student data by cloud vendors
Defines "student data"
Requires cloud providers to certify in writing that they comply with the KRS

House Bill 5 (2014)
Called for the creation of KRS 61.931, 61.932 and 61.933 (See Appendix A)
Defines "Personal Information" or "PII"
Requires school districts to establish "reasonable security and breach investigation procedures and practices"
Outlines security breach notification procedures and timelines

702 KAR 1:170 (2015)
Authorized by House Bills 5 and 232 (See Appendix A)
Requires that the district acknowledge to its local board prior to August 31 of each year that it has reviewed the guidance of the KAR and implemented best practices

Data Security and Breach Notification Best Practices Guide

See Appendix A

Main Causes of Data Breaches

- Accidental Sharing (email, website, paper)
- Weak or stolen passwords
- Loss/Theft of device
- Phishing
- Malware
- Application vulnerabilities
- Hackers

Current Spencer County Measures to Prevent a Breach

- Anti-Virus/Malware/Spam/Spyware Protection
- Vulnerability Scanning
- System Patch Management
- Active Directory/Group Policy Objects
- Private IP implementation
- Distributed Denial of Service (DDOS) Mitigation
- Web Filtration
- Centrally Managed Firewalls
- Virtual Private Network Support
- Secure File Transfer
- Statewide Product Standards
- Locked Data Center
- Forced workstation restarts
- Device screen time outs
- Limit access to data based on job requirements
- Consistent review of processes for account creation/deletion and access to data
- Mandatory password changes (complex) for all staff twice per school year
- Training/Communications for all district employees via email and/or Administrator meetings
- Purchasing process requires cloud providers to comply with KRS 365.734 (House Bill 232 which prohibits certain uses of student data by cloud vendors)
- Multi Factor Authentication for all staff
- Conditional Access
- Self Service Password Reset
- Surveillance cameras

Summary

It is our intent to continue due diligence in protecting data that relates to staff, students, and the operations of Spencer County Schools.

Appendix A

702 KAR 1:170. School district data security and breach procedures.

RELATES TO: KRS 61.931, 61.932, 61.933
STATUTORY AUTHORITY: KRS 61.932(1)(b), 156.070
NECESSITY, FUNCTION AND CONFORMITY: KRS 156.070 authorizes the Kentucky Board of Education (KBE) to promulgate administrative regulations necessary for the efficient management, control, and operation of the schools and programs under its jurisdiction. KRS 61.932(1)(b) specifically requires the KBE to promulgate administrative regulations establishing requirements and standards for the reasonable security and breach investigation procedures and practices established and implemented by public school districts. This administrative regulation establishes the requirements and standards for school district reasonable security and breach investigation procedures and practices.

Section 1. Definitions. (1) "Personal information" is defined by KRS 61.931(6).
(2) "Reasonable security and breach investigation procedures and practices" is defined by KRS 61.931(8).

Section 2. Best Practice Guide for School District Personal Information Reasonable Security. The department shall at least annually provide school districts best practice guidance for personal information reasonable security. The current department guidance is provided in the Data Security and Breach Notification Best Practice Guide, which is incorporated by reference into this administrative regulation. School districts shall not be required to adopt the security practices included in this guidance.

Section 3. Annual Public School District Acknowledgement of Best Practices. Each public school district shall review and consider, in light of the needs of reasonable security, the most recent best practice guidance, including the Data Security and Breach Notification Best Practice Guide, for personal information reasonable security. Each public school district shall acknowledge to its own local board during a public board meeting prior to August 31 of each year, that the district has reviewed this guidance and implemented the best practices that meet the needs of personal information reasonable security in that district.

Section 4. Annual Department Acknowledgement of Best Practices. The department shall review and consider, in light of the needs of reasonable security, the most recent best practice guidance for personal information reasonable security. The department shall acknowledge to the KBE, by August 31 of each year, that the department has reviewed this guidance and implemented the best practices that meet the needs of personal information reasonable security for the department.

Section 5. Data Breach Notification to the Department. Any public school district that determines or is notified of a security breach relating to personal information collected, maintained, or stored by the school district or by a nonaffiliated third party on behalf of the school district shall provide the notification of the security breach to the department required by KRS 61.933, pursuant to the procedure included in the Data Security and Breach Notification Best Practice Guide.

Section 6. Incorporation by Reference. (1) "Data Security and Breach Notification Best Practice Guide", September 2015, is incorporated by reference.
(2) This material may be inspected, copied, or obtained, subject to applicable copyright law,

at the Department of Education, 500 Mero Street, First Floor, Capital Plaza Tower, Frankfort, Kentucky 40601, Monday through Friday, 8 a.m. to 4:30 p.m. (42 Ky.R. 1069; 1735; eff. 1-4-2016.)

160.700 Definitions related to KRS 160.700 to 160.730.

As used in this chapter, unless the context otherwise requires:

(1) "Directory information" means the student's name, address, telephone listing, date and place of birth, participation in school recognized sports and activities, height and weight of members of athletic teams, dates of attendance, awards received, major field of study, and the most recent previous educational agency or institution attended by the student, contained in education records in the custody of the public schools;

(2) "Educational institution" means any public school providing an elementary and secondary education, including vocational;

(3) "Education record" means data and information directly relating to a student that is collected or maintained by educational institutions or by a person acting for an institution including academic records and portfolios; achievement tests; aptitude scores; teacher and counselor evaluations; health and personal data; behavioral and psychological evaluations; and directory data recorded in any medium including handwriting, magnetic tapes, film, video, microfiche, computer-generated and stored data, or data otherwise maintained and used by the educational institution or a person acting for an institution. "Education record" shall not include:

   (a) Records of instructional, supervisory, and assisting administrative personnel which are in the sole possession of the maker and are not accessible or revealed to any other person except a substitute for any of those persons;

   (b) Records maintained by a law enforcement unit of the educational institution that were created by that law enforcement unit for the purpose of law enforcement;

   (c) In the case of persons who are employed by an educational agency or institution but who are not in attendance at that agency or institution, records made and maintained in the normal course of business which relate exclusively to that person in the person's capacity as an employee and are not available for use for any other purpose; or

   (d) Records on a student who is eighteen (18) years of age or older, which are made, used, or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional for treatment of the student, and are not available to anyone other than persons providing this treatment, except a physician or other appropriate professional of the student's choice.

(4) "Eligible student" means a student, or a former student, who has reached the age of eighteen (18) or is pursuing an education beyond high school and therefore the permission or consent required of, and the rights accorded to the parents of the student shall thereafter be required of, and accorded to the student;

(5) "School official" means personnel employed in instructive and administrative positions with a school board or educational institution. Parents and other non-educational persons who are elected or appointed to school-based decision making councils or committees thereof, or other voluntary boards or committees shall not be considered school officials.

Effective: July 15, 1994

History: Created 1994 Ky. Acts ch. 98, sec. 1, effective July 15, 1994

61.931 Definitions for KRS 61.931 to 61.934.

As used in KRS 61.931 to 61.934:

(1) "Agency" means:

(a) The executive branch of state government of the Commonwealth of Kentucky;

(b) Every county, city, municipal corporation, urban-county government, charter county government, consolidated local government, and unified local government;

(c) Every organizational unit, department, division, branch, section, unit, office, administrative body, program cabinet, bureau, board, commission, committee, subcommittee, ad hoc committee, council, authority, public agency, instrumentality, interagency body, special purpose governmental entity, or public corporation of an entity specified in paragraph (a) or (b) of this subsection or created, established, or controlled by an entity specified in paragraph (a) or (b) of this subsection;

(d) Every public school district in the Commonwealth of Kentucky; and

(e) Every public institution of postsecondary education, including every public university in the Commonwealth of Kentucky and public college of the entire Kentucky Community and Technical College System;

(2) "Commonwealth Office of Technology" means the office established by KRS 42.724;

(3) "Encryption" means the conversion of data using technology that:

(a) Meets or exceeds the level adopted by the National Institute of Standards Technology as part of the Federal Information Processing Standards: and

(b) Renders the data indecipherable without the associated cryptographic key to decipher the data;

(4) "Law enforcement agency" means any lawfully organized investigative agency, sheriff's office, police unit, or police force of federal, state, county, urban-county government, charter county, city, consolidated local government, unified local government, or any combination of these entities, responsible for the detection of crime and the enforcement of the general criminal federal and state laws;

(5) "Nonaffiliated third party" means any person that:

(a) Has a contract or agreement with an agency; and

(b) Receives personal information from the agency pursuant to the contract or agreement;

(6) "Personal information" means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

(a) An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;

(b) A Social Security number;

(c) A taxpayer identification number that incorporates a Social Security number;

(d) A driver's license number, state identification card number, or other individual identification number issued by any agency;

(e) A passport number or other identification number issued by the United States government; or

(f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g;

(7) (a) "Public record or record," as established by KRS 171.410, means all books, papers, maps, photographs, cards, tapes, disks, diskettes, recordings, and other documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of, or retained by a public agency.

(b) "Public record" does not include any records owned by a private person or corporation that are not related to functions, activities, programs, or operations funded by state or local authority;

(8) "Reasonable security and breach investigation procedures and practices" means data security procedures and practices developed in good faith and set forth in a written security information policy; and

(9) (a) "Security breach" means:

1. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals; or

2. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises or the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals.

(b) "Security breach" does not include the good-faith acquisition of personal information by an employee, agent, or nonaffiliated third party of the agency for the purposes of the agency if the personal information is used for a purpose related to the agency and is not subject to unauthorized disclosure.

Effective: January 1, 2015

History: Created 2014 Ky. Acts ch. 74, sec. 1, effective January 1, 2015.

Legislative Research Commission Note (1/1/2015). 2014 Ky. Acts ch. 74, sec. 10 provided that "the provisions of this Act shall not impact the provisions of KRS 61.870 to 61.884." That proviso applies to this statute as created in Section 1 of that Act.

365.734 Prohibited uses of personally identifiable student information by cloud computing service provider -- Administrative regulations.

(1) As used in this section:

(a) "Cloud computing service" means a service that provides, and that is marketed and designed to provide, an educational institution with account-based access to online computing resources;

(b) "Cloud computing service provider" means any person other than an educational institution that operates a cloud computing service;

(c) "Educational institution" means any public, private, or school administrative unit serving students in kindergarten to grade twelve (12);

(d) "Person" means an individual, partnership, corporation, association, company, or any other legal entity;

(e) "Process" means to use, access, collect, manipulate, scan, modify, analyze, transform, disclose, store, transmit, aggregate, or dispose of student data; and

(f) "Student data" means any information or material, in any medium or format, that concerns a student and is created or provided by the student in the course of the student's use of cloud computing services, or by an agent or employee of the educational institution in connection with the cloud computing services. Student data includes the student's name, e-mail address, e-mail messages, postal address, phone number, and any documents, photos, or unique identifiers relating to the student.

(2) A cloud computing service provider shall not process student data for any purpose other than providing, improving, developing, or maintaining the integrity of its cloud computing services, unless the provider receives express permission from the student's parent. However, a cloud computing service provider may assist an educational institution to conduct educational research as permitted by the Family Educational Rights and Privacy Act of 1974, as amended, 20 U.S.C. sec. 1232g. A cloud computing service provider shall not in any case process student data to advertise or facilitate advertising or to create or correct an individual or household profile for any advertisement purpose, and shall not sell, disclose, or otherwise process student data for any commercial purpose.

(3) A cloud computing service provider that enters into an agreement to provide cloud computing services to an educational institution shall certify in writing to the educational institution that it will comply with subsection (2) of this section.

(4) The Kentucky Board of Education may promulgate administrative regulations in accordance with KRS Chapter 13A as necessary to carry out the requirements of this section.

Effective: July 15, 2014

History: Created 2014 Ky. Acts ch. 84, sec. 2, effective July 15, 2014.

61.932 Personal information security and breach investigation procedures and practices for certain public agencies and nonaffiliated third parties.

(1) (a) An agency or nonaffiliated third party that maintains or otherwise possesses personal information, regardless of the form in which the personal information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches.

(b) Reasonable security and breach investigation procedures and practices established and implemented by organizational units of the executive branch of state government shall be in accordance with relevant enterprise policies established by the Commonwealth Office of Technology. Reasonable security and breach investigation procedures and practices established and implemented by units of government listed under KRS 61.931(1)(b) and (c) that are not organizational units of the executive branch of state government shall be in accordance with policies established by the Department for Local Government. The Department for Local Government shall consult with public entities as defined in KRS 65.310 in the development of policies establishing reasonable security and breach investigation procedures and practices for units of local government pursuant to this subsection. Reasonable security and breach investigation procedures and practices established and implemented by public school districts listed under KRS 61.931(1)(d) shall be in accordance with administrative regulations promulgated by the Kentucky Board of Education. Reasonable security and breach investigation procedures and practices established and implemented by educational entities listed under KRS 61.931(1)(e) shall be in accordance with policies established by the Council on Postsecondary Education. The Commonwealth Office of Technology shall, upon request of an agency, make available technical assistance for the establishment and implementation of reasonable security and breach investigation procedures and practices.

(c) 1. If an agency is subject to any additional requirements under the Kentucky Revised Statutes or under federal law, protocols, or agreements relating to the protection and privacy of personal information, the agency shall comply with these additional requirements, in addition to the requirements of KRS 61.931 to 61.934.

2. If a nonaffiliated third party is required by federal law or regulation to conduct security breach investigations or to make notifications of security breaches, or both, as a result of the nonaffiliated third party's unauthorized disclosure of one (1) or more data elements of personal information that is the same as one (1) or more of the data elements of personal information listed in KRS 61.931(6)(a) to (f), the nonaffiliated third party shall meet the requirements of KRS 61.931 to 61.934 by providing to the agency a copy of any and all reports and investigations relating to such security breach investigations or notifications that are required to be made by federal law or regulations. This subparagraph

shall not apply if the security breach includes the unauthorized disclosure of data elements that are not covered by federal law or regulation but are listed in KRS 61.931(6)(a) to (f).

(2) (a) For agreements executed or amended on or after January 1, 2015, any agency that contracts with a nonaffiliated third party and that discloses personal information to the nonaffiliated third party shall require as part of that agreement that the nonaffiliated third party implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices referenced in subsection (1)(b) of this section, and that are reasonably designed to protect the personal information from unauthorized access, use, modification, disclosure, manipulation, or destruction.

(b) 1. A nonaffiliated third party that is provided access to personal information by an agency, or that collects and maintains personal information on behalf of an agency shall notify the agency in the most expedient time possible and without unreasonable delay but within seventy-two (72) hours of determination of a security breach relating to the personal information in the possession of the nonaffiliated third party. The notice to the agency shall include all information the nonaffiliated third party has with regard to the security breach at the time of notification. Agreements referenced in paragraph (a) of this subsection shall specify how the cost of the notification and investigation requirements under KRS 61.933 are to be apportioned when a security breach is suffered by the agency or nonaffiliated third party.

2. The notice required by subparagraph 1. of this paragraph may be delayed if a law enforcement agency notifies the nonaffiliated third party that notification will impede a criminal investigation or jeopardize homeland or national security. If notice is delayed pursuant to this subparagraph, notification shall be given as soon as reasonably feasible by the nonaffiliated third party to the agency with which the nonaffiliated third party is contracting. The agency shall then record the notification in writing on a form developed by the Commonwealth Office of Technology that the notification will not impede a criminal investigation and will not jeopardize homeland or national security. The Commonwealth Office of Technology shall promulgate administrative regulations under KRS 61.931 to 61.934 regarding the content of the form.

Effective: January 1, 2015

History: Created 2014 Ky. Acts ch. 74, sec. 2, effective January 1, 2015.

Legislative Research Commission Note (1/1/2015). 2014 Ky. Acts ch. 74, sec. 10 provided that "the provisions of this Act shall not impact the provisions of KRS 61.870 to 61.884." That proviso applies to this statute as created in Section 2 of that Act.

61.933 Notification of personal information security breach -- Investigation -- Notice to affected individuals of result of investigation -- Personal information not subject to requirements -- Injunctive relief by Attorney General.

(1) (a) Any agency that collects, maintains, or stores personal information that determines or is notified of a security breach relating to personal information collected, maintained, or stored by the agency or by a nonaffiliated third party on behalf of the agency shall as soon as possible, but within seventy-two (72) hours of determination or notification of the security breach:

1. Notify the commissioner of the Kentucky State Police, the Auditor of Public Accounts, and the Attorney General. In addition, an agency shall notify the secretary of the Finance and Administration Cabinet or his or her designee if an agency is an organizational unit of the executive branch of state government; notify the commissioner of the Department for Local Government if the agency is a unit of government listed in KRS 61.931(1)(b) or (c) that is not an organizational unit of the executive branch of state government; notify the commissioner of the Kentucky Department of Education if the agency is a public school district listed in KRS 61.931(1)(d); and notify the president of the Council on Postsecondary Education if the agency is an educational entity listed under KRS 61.931(1)(e). Notification shall be in writing on a form developed by the Commonwealth Office of Technology. The Commonwealth Office of Technology shall promulgate administrative regulations under KRS 61.931 to 61.934 regarding the contents of the form; and
2. Begin conducting a reasonable and prompt investigation in accordance with the security and breach investigation procedures and practices referenced in KRS 61.932(1)(b) to determine whether the security breach has resulted in or is likely to result in the misuse of the personal information.

(b) Upon conclusion of the agency's investigation:

1. If the agency determined that a security breach has occurred and that the misuse of personal information has occurred or is reasonably likely to occur, the agency shall:
   a. Within forty-eight (48) hours of completion of the investigation, notify in writing all officers listed in paragraph (a)1. of this subsection, and the commissioner of the Department for Libraries and Archives, unless the provisions of subsection (3) of this section apply;
   b. Within thirty-five (35) days of providing the notifications required by subdivision a. of this subparagraph, notify all individuals impacted by the security breach as provided in subsection (2) of this section, unless the provisions of subsection (3) of this section apply; and

c. If the number of individuals to be notified exceeds one thousand (1,000), the agency shall notify, at least seven (7) days prior to providing notice to individuals under subdivision b. of this subparagraph, the Commonwealth Office of Technology if the agency is an organizational unit of the executive branch of state government, the Department for Local Government if the agency is a unit of government listed under KRS 61.931(1)(b) or (c) that is not an organizational unit of the executive branch of state government, the Kentucky Department of Education if the agency is a public school district listed under KRS 61.931(1)(d), or the Council on Postsecondary Education if the agency is an educational entity listed under KRS 61.931(1)(e); and notify all consumer credit reporting agencies included on the list maintained by the Office of the Attorney General that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. sec. 1681a(p), of the timing, distribution, and content of the notice; or

2. If the agency determines that the misuse of personal information has not occurred and is not likely to occur, the agency is not required to give notice, but shall maintain records that reflect the basis for its decision for a retention period set by the State Archives and Records Commission as established by KRS 171.420. The agency shall notify the appropriate entities listed in paragraph (a)1. of this subsection that the misuse of personal information has not occurred.

(2) (a) The provisions of this subsection establish the requirements for providing notice to individuals under subsection (1)(b)1.b. of this section. Notice shall be provided as follows:

1. Conspicuous posting of the notice on the Web site of the agency;

2. Notification to regional or local media if the security breach is localized, and also to major statewide media if the security breach is widespread, including broadcast media, such as radio and television; and

3. Personal communication to individuals whose data has been breached using the method listed in subdivision a., b., or c. of this subparagraph that the agency believes is most likely to result in actual notification to those individuals, if the agency has the information available:

a. In writing, sent to the most recent address for the individual as reflected in the records of the agency;

b. By electronic mail, sent to the most recent electronic mail address for the individual as reflected in the records of the agency, unless the individual has communicated to the agency in writing that they do not want email notification; or

c. By telephone, to the most recent telephone number for the individual as reflected in the records of the agency.

(b) The notice shall be clear and conspicuous, and shall include:

1. To the extent possible, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired;
2. Contact information for the notifying agency, including the address, telephone number, and toll-free number if a toll-free number is maintained;
3. A description of the general acts of the agency, excluding disclosure of defenses used for the protection of information, to protect the personal information from further security breach; and
4. The toll-free numbers, addresses, and Web site addresses, along with a statement that the individual can obtain information from the following sources about steps the individual may take to avoid identity theft, for:
   a. The major consumer credit reporting agencies;
   b. The Federal Trade Commission; and
   c. The Office of the Kentucky Attorney General.

(c) The agency providing notice pursuant to this subsection shall cooperate with any investigation conducted by the agencies notified under subsection (1)(a) of this section and with reasonable requests from the Office of Consumer Protection of the Office of the Attorney General, consumer credit reporting agencies, and recipients of the notice, to verify the authenticity of the notice.

(3) (a) The notices required by subsection (1) of this section shall not be made if, after consultation with a law enforcement agency, the agency receives a written request from a law enforcement agency for a delay in notification because the notice may impede a criminal investigation. The written request may apply to some or all of the required notifications, as specified in the written request from the law enforcement agency. Upon written notification from the law enforcement agency that the criminal investigation has been completed, or that the sending of the required notifications will no longer impede a criminal investigation, the agency shall send the notices required by subsection (1)(b)1. of this section.

(b) The notice required by subsection (1)(b)1.b. of this section may be delayed if the agency determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented within the timeframe established by subsection (1)(b)1.b. of this section, and the delay is approved in writing by the Office of the Attorney General. If notice is delayed pursuant to this subsection, notice shall be made immediately after actions necessary to restore the integrity of the data system have been completed.

(4) Any waiver of the provisions of this section is contrary to public policy and shall be void and unenforceable.

(5) This section shall not apply to:

(a) Personal information that has been redacted;

(b) Personal information disclosed to a federal, state, or local government entity, including a law enforcement agency or court, or their agents, assigns, employees, or subcontractors, to investigate or conduct criminal investigations and arrests or delinquent tax assessments, or to perform any other statutory duties and responsibilities;

(c) Personal information that is publicly and lawfully made available to the general public from federal, state, or local government records;

(d) Personal information that an individual has consented to have publicly disseminated or listed; or

(e) Any document recorded in the records of either a county clerk or circuit clerk of a county, or in the records of a United States District Court.

(6) The Office of the Attorney General may bring an action in the Franklin Circuit Court against an agency or a nonaffiliated third party that is not an agency, or both, for injunctive relief, and for other legal remedies against a nonaffiliated third party that is not an agency to enforce the provisions of KRS 61.931 to 61.934. Nothing in KRS 61.931 to 61.934 shall create a private right of action.

Effective: January 1, 2015

History: Created 2014 Ky. Acts ch. 74, sec. 3, effective January 1, 2015.

Legislative Research Commission Note (1/1/2015). 2014 Ky. Acts ch. 74, sec. 10 provided that "the provisions of this Act shall not impact the provisions of KRS 61.870 to 61.884." That proviso applies to this statute as created in Section 3 of that Act.

Legislative Research Commission Note (1/1/2015). In codification, the Reviser of Statutes has corrected a manifest clerical or typographical error in subsection (1)(a)1. of this statute by changing a reference to the educational entity agencies that must notify the president of the Council on Postsecondary Education of a security breach that are listed in "subsection (1)(c) of Section 1 of this Act" (KRS 61.931) to "subsection (1)(e) of Section 1 of this Act," making the reference once codified read "KRS 61.931(1)(e)."

Legislative Research Commission Note (1/1/2015). In codification, the Reviser of Statutes has corrected a manifest clerical or typographical error in subsection (1)(a)2. of this statute by changing a reference to the security and breach investigation procedures and practices referenced in "subsection (1)(b) of this section" to "subsection (1)(b) of Section 2 of this Act," making the reference once codified read "KRS 61.932(1)(b)."

Data Security and Breach Notification Best Practice Guide

Kentucky Department of Education (KDE)

V2.2 September 2015

Kentucky Department of Education
300 Sower Blvd.
Frankfort, KY 40601
(502) 564-2020

Special Note:

This guide is a living document and subject to change. Districts will be alerted to major changes, which could occur at any time. Otherwise, updates to this document will be available each August.

Version Control

Version	Date	Author	Change Description
2.0	4/22/2015	R. Hackworth	Adapted from 2006 HB 341 Data Security Study
2.1	4/24/2015	R. Hackworth	Added “version control.” Added “Resources” section with webcast archive & COT document links at end of document. Changed links for HBs 5 and 232 docs to highlighted versions used during noted webcast.
2.2	7/20/2015	R. Hackworth	Added data breach notification distribution list

Overview

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 intent of the study requested by the legislature was to provide some general guidelines and recommendations to KDE and school districts related to some basic measures that can be considered to protect and prevent the access to restricted personal information by any person that does not have the proper access rights, authority or the "need to know" (a.k.a., an unauthorized person) and to provide some considerations and protocols in regards to notifying any affected individual should this type of information be made available in paper or electronic form to any unauthorized person.

Since that legislation, the threat and occurrence of data breaches has only increased. The House Bill 341 data security study has remained an effective cornerstone of guidance, and new legislation has added clarity, definition, and direction. But, as technology and how we use it in the schools has changed, so must that original guidance. This document, while incorporating the still-relevant guidance of the HB 341 study, will supersede it.

One thing that has not changed, however, is KDE's role. Since the Kentucky Educational Technology System (KETS) began in the early 1990s, districts have possessed the authority and responsibility to ensure their own security, whether it be part of the network, data system or even paper documents on a desk. KIDS does not have the staff or desire to begin inspecting, approving, disapproving, or monitoring each district's reasons or detailed actions in implementing or not implementing suggested best practices. However KIDS staff will be a resource for any questions or suggestions for additions/edits a district has throughout the years in regards to the reg and the best practice guideline. Any district wanting anything beyond that (e.g., an annual inspection, confirmation, thumbs up of their data security, a professional opinion on which data security recommendations should or shouldn't be implemented within their district, etc) will be pointed to resources outside of KDE (see "Remediation, below) that can best help them with the types of task/services.

On January 1, 2015, a new state law, the Personal Information Security and Breach Investigation Procedures and Practices Act (KRS 61.931, et seq.) went into effect. This legislation is more commonly known as "House Bill 5." This Act concerns the protection of personal information and applies to every state agency, including KDE, every public school district, and every vendor with which we have contracts. While this document incorporates best practice that we are all encouraged to follow, it also incorporates the "have to" actions from KRS 61.931, et seq. (HB 5).

In addition to the legal requirements, this document makes recommendations based on research and experience (best practice). However, there is no guarantee that implementing all of the recommendations will remove 100% of the risk of a data breach. Each district is encouraged to implement the recommendations that it believes are the most helpful given its perception of risk and fiscal capabilities.

This next section provides a summary of the requirements, prior to and following a suspected or confirmed data breach, from KRS 61.931, et seq. (HB 5). The remaining sections either provide more detail for these requirements or provide recommendations.

Data Breach Act "Have to" Section

Please be advised that this is a summary. A thorough understanding of KRS 61.931, et seq. (HB 5), along with its included definitions, will be very helpful and is recommended.

Immediately

- Procedures and practices to safeguard against security breaches must be implemented by any entity that maintains or possesses personal information in accordance with applicable KRS and federal laws.
- For any contracts involving personal information that are entered into or amended after January 1st, 2015, specific language requiring protection of the data must be included.

Within 72 Hours of Suspected or Confirmed Breach

1. Send notification, via the FAC-001 form, to the Department via email at KDE Data Breach Notification and to the following agencies as required by KRS 61.933:
    a. Attorney General's Office
    b. Auditor of Public Accounts
    c. Finance and Administration Cabinet
    d. Kentucky State Police
    e. Kentucky Department of Library and Archives
    f. Commonwealth Office of Technology

    Upon notification to the Department at the KDE Data Breach Notification email, the Department shall provide the school district the most current contact information for the notification to the other agencies required by KRS 61.933. If there is an ongoing investigation involving law enforcement which prevents information being disclosed to the Department, use the FAC-002 form to provide the notification required by KRS 61.933.
2. Begin conducting a "reasonable and prompt" investigation to determine "whether the security breach has resulted in or is likely to result in the misuse of personal information."

Within 48 Hours of Completion of the Investigation

Notify the above staff contacts if the investigation finds that the misuse of personal information has occurred or is likely to occur. The length of the investigation is not set, and will vary with each instance.

Within 35 Days of Suspected or Confirmed Breach

- Notify all individuals impacted by the breach in a manner required by KRS 61.931, et seq. including information required by the Act. If breach impacts more than 1,000 individuals, nationwide consumer reporting agencies must also be notified. KDE recommends notifying affected individuals as soon as possible and not waiting until the 35th day.
- If the investigation determines that misuse of personal information has not occurred or is not likely to occur, notification of the impacted individuals is not required, but records of the decision and evidence must be kept. Notification of the agency contacts, above, is still required noting that misuse of personal information has NOT occurred.

Data at Risk

Unlike the private sector or most other parts of government, a very high percentage of the data elements collected and used in P-12 schools are not considered confidential and are usually made directly accessible to any public citizen either instantly through a variety of electronic means (e.g., Web sites at schools, district offices, the Kentucky Department of Education and the U.S. Education Department) or very quickly in response to open records requests that must be provided in paper or e-mail form. Also, most of the data collected at the state and federal level are in summative form and therefore do not contain individually identifiable or confidential data.

This means that access to the majority of the truly private P-12 data is controlled by district staff, who control the permissions to these areas, systems and services. Most reside physically (e.g., on paper within cabinets, on electronic files inside a fileserver or workstation) within the district though as cloud services increase in popularity, more and more sensitive or confidential data exists outside of the district boundaries, though still under district control.

There is a category of P-12 data that is considered very personal and restricted and is becoming more and more sought after by identity thieves – the social security numbers of students. Even more than the SSNs of adults, the SSNs of children are valuable because children usually do not engage in behavior that might result in a credit check. This means the identity thief can use or sell these SSNs for years before ever having any attention drawn to them.

Most of the time, if there is an exposure of this type of restricted personal data, such as a student's medical records or a teacher's SSN, it happens accidentally (e.g., confidential personal data is printed to an unintended printer in a building, e-mailed to the wrong person or group or placed on an incorrect Web site). Also, the number of people who accidentally see confidential data that they should not be viewing tends to be limited to a small group; most of which disregard or destroy what they have seen because they do not realize that it is restricted personal data.

Yet, there are times where there are intentional attempts (e.g., a laptop or cabinet drawer containing paper files is stolen from a school, someone is just curious about a fellow employee's personal information) to access restricted personal information by unauthorized people who do not have a true need to know.

Whether the exposure happens accidentally or intentionally, the same prevention steps and notification protocols should be considered for all restricted personal data, no matter the media form (i.e. paper or electronic) that that data is stored on. In fact, most organizations already have well-established procedures for confidential personal data that is on paper form, which also can be considered for the same type of restricted data that is available and stored in electronic form.

The bottom line is that pre-emptive measures to protect and prevent the access by unauthorized people should be taken by each P-12 organization that controls and manages restricted personal information. However, if an individual's restricted personal information possibly has been seen by an unauthorized person, no matter how small or large the level of knowledgeable exposure, there is an obligation to let the affected individual know as quickly as possible that restricted personal data may have been compromised and disclosed to unauthorized people. If possible, that affected person should be informed what specific restricted data has been exposed, how long it has been exposed, who it has been exposed to and how the exposure occurred. This must be done no matter how embarrassing this announcement may be to the organization that is responsible for that restricted data becoming accidentally exposed or a victim of its data system being successfully accessed through criminal activity.

The Three Major Areas of Consideration of Personal Data Security Management

This study was originally conducted by Kentucky Department of Education with research derived from information received from Gartner, NOREX and various state departments around the nation. Gartner provides independent research and analysis to private and public organizations over a wide range of technology subjects. Norex is a consortium of public and private companies that share their policies, lessons learned and processes with the other association members to consider for use in their organizations. Finally, a large number of states already have established legislation and policies that we can learn from without trying to reinvent the wheel. Therefore, we considered and consolidated information gathered from all these sources into a concise report that focuses on three major areas:

- Protection and Prevention
- Preparation for Notification
- Notification

1. Protection and Prevention

Organizations must implement an effective incident response program that includes pre-incident preparation; detection and analysis; containment; mitigation and recovery; and post-incident activities. Proper preparation (e.g. staff education, a healthy data diet) and awareness of legal and ethical issues are crucial.

The level of acceptable risk should be articulated, and security procedures should be balanced with available funding for information and data security, access and safeguards. In the event that more secure measures are needed, these measures should be identified for implementation and allocation of resources.

The cornerstone of improving data security is basic awareness among all staff. To promote awareness of data security best practices, the Kentucky Department of Education's Data Governance team has produced a series of three short videos focused on protecting personal information. While everyone is welcome to view and use these videos, please keep in mind they were developed specifically for KDE use and may not perfectly match every district's needs.

1. What is PII?
2. Data Access and Sharing
3. Was that a Data Breach?

Additional information about data privacy and security from KDE, the U.S. Education Department, PTAC, and others can be found on the KDE website here.

An organization should protect the confidentiality of personal information whether it pertains to customers, employees, parents or students. For both paper and electronic records, these components include physical, technical and administrative safeguards. Among such safeguards are the following recommended practices:

- **Do the Basics** – Keep and promote awareness of basic, but extremely important, security and privacy policies related to
    - using strong passwords or passphrases and changing them often,
    - keeping a password, PIN or passcode on all devices, including laptops, tablets and smartphones,
    - whenever staff depart:
        - changing security entry codes/locks for buildings/rooms containing sensitive information
        - removing old or unused user accounts from all systems
    - ongoing employee training and communications.

  This should help reduce the number of incidences or magnitude of exposure of very sensitive data, while at the same time increasing the speed of proper notification and protocol should this exposure occur.
- **Keep Accurate and Updated Data Inventories** - Inventory all of your records systems (e.g., electronic and paper storage media) to identify those containing any type of personal information. This will help you decide what level of protection is necessary for each system, and what priority it has in your educational processes.
- **Have a Healthy Data Diet** - Collect the minimum amount of personal information necessary to accomplish your educational purposes, and retain it for the minimum time necessary.
- **Classify Data** - Classify information in each paper and electronic records system according to sensitivity and the level of risk if that information was accidentally or intentionally accessed by anyone without a need to know. A simple rule of thumb that can be used to quickly identify the data that has the highest levels of sensitivity and confidentiality in an organization would be to reflect on whether the data could be posted on a public website or viewed by anyone making an open records request.
- **Intruder Detection** - Use appropriate physical and technological safeguards, such as video surveillance or alarms on buildings or rooms, to protect personal information, particularly higher-risk information, in paper as well as electronic records.
- **Vendor Management** - Require service providers and educational partners who handle personal information on behalf of your organization to follow your security policies and procedures as well as state and federal laws (such as HBs 5, 232 and COPPA). KDE has developed the following verbiage, which, if used by any district, must be customized, for inclusion in contracts:
    - KDE RFP Attachment - Data Security and Breach Protocols
    - KDE RFP Attachment - FERPA and Affidavit of Non-Disclosure
- **Encryption** - Wherever it makes sense, such as devices used to host or access high-risk information, use data encryption in combination with host protection and access control. Pay particular attention to protecting higher-risk personal information on laptops and other portable computers and mobile storage devices (e.g. smartphones, CDs, thumb drives).
- **Records Retention** - Dispose of records and equipment containing personal information in a secure manner.
- **Document Your Security** - Have a security plan and review it at least annually or whenever there is a material change in educational practices, delivery mechanism, where the data is stored and how it accessed that may reasonably implicate the security of sensitive personal information.

2. Preparation for Notification of Affected Individuals

- **Leading the Charge** - Designate an individual, such as the CIO, as responsible for coordinating your internal investigation and notification procedures for the paper and electronic restricted personal data for which you are responsible.
- **Data Breach Policy** - Outline investigation and notification procedures to be followed if the school district determines or is notified of a security breach of personal information, including notice to the individual whose personal information was breached or to the parents of an individual under eighteen (18) years of age whose personal information was breached, documentation of the event, and a process for the parents or individual to request a debriefing session regarding the breach.
    - Consider suggestions from law enforcement with expertise in investigating crimes that use technology (e.g., hackers breaking into fileservers) and nontechnology (e.g., burglars breaking into buildings) means for intentionally accessing unauthorized restricted personal information for inclusion in your incident response plan.
    - Consider suggestions from your legal staff during planning. They have the greatest knowledge and expertise on what data does and does not meet the requirements of the open records law. This means they can be very valuable in helping you identify the most restricted personal data in your organization. They also can help you craft the wording for your written or verbal notifications that must be provided when an exposure occurs. They can point you to the most appropriate law enforcement official to contact should criminal activity be the reason the data became exposed or if the exposed data is possibly being used for criminal purposes (e.g., identity theft, fraud).
    - Adopt written procedures, in accordance with data breach legislation, for notification of individuals whose unencrypted notice-triggering personal information have been, or are reasonably believed to have been, acquired by an unauthorized person. Notification can take many forms that include a face-to-face meeting, a phone call, posting on a Web site or sending a paper notice to each affected person's home. The number of people that need to be contacted will usually influence the form of notification that is chosen and how quickly each person can be reasonably notified
- **Training** - Regularly train employees, including all new, temporary and contract employees, in their roles and responsibilities in your data breach policy/incident response plan. It is also important to make sure everyone is familiar with key terms such as "confidential," "PII," and what, exactly, defines a breach.
- **Remediation** - In addition to the notification of state agencies, each district, just like KDE, is expected to be able to remediate the issue which allowed the breach to occur. Plan for and use measures to contain, control and correct any security incident that may involve higher-risk personal information. Multiple options are available.
    - Many IT auditing firms can offer forensic/recovery/notification services in addition to pre-incident vulnerability auditing for potential weaknesses. Districts are encouraged to inquire with their existing auditors for these services.
    - Check the Best Practice Guidelines page on the KDE website for the current state contract holder for security services, including vulnerability assessment and forensic investigations.

    - Also check with other state contract holders, such as for anti-virus products, which may provide additional security services and also be helpful.
    - The Commonwealth Office of Technology also offers various security services available to all state agencies and public school districts.
    - The United States Computer Emergency Readiness Team (US-CERT) offers a free or facilitated Cyber Resilience Review "to evaluate an organization's operational resilience and cybersecurity practices."
- **Whom to Call** - Identify appropriate law enforcement contacts to notify on security incidents that may involve illegal activities. Keep important numbers handy.
- **Documentation** – As soon as a potential breach occurs, it is important to document the issues found and response actions taken on an incident.

Reflect and Review - Review your incident response plan at least annually or whenever there is a significant change in your educational practices or how the data can be accessed electronically or in paper form. It is also important, after a security incident, to reflect on what worked well, and perhaps not so well, and then make changes to your process.

3. Notification

As of January 1st, 2015, Kentucky began to require notification of suspected or confirmed data breaches. With the passage of KRS 61.931, ET SEQ. (HB 5), Kentucky public agencies and public schools are required to notify both the individual victims of a breach and various state officials.

House Bill 5 addresses the safety and security of personal information held by public agencies and requires public agencies and nonaffiliated third parties to implement, maintain, and update security procedures and practices, including taking any appropriate corrective action to safeguard against security breaches.

- House Bill 5 document with Highlighting

House Bill 232 has two sections. Section 1 requires consumer notification when a private party data breach reveals personally identifiable information. Section 2 requires cloud computing service providers contracting with educational institutions to maintain security of student data.

- House Bill 232 document with Highlighting

In addition to this legislation, districts are encouraged to review the following links, which provide helpful information regarding contractual arrangements with cloud service providers:

- Gartner insights: 3 important questions to ask your potential cloud provider
- Infoworld – Gartner: Seven cloud-computing security risks
- Gartner: Cloud Exit Strategies

Required Data Breach Notification Forms

As noted in House Bill 5, the following forms, developed by the Commonwealth Office of Technology, are to be used to notify all required agencies in the event of a breach or a suspected breach of data.

- Data Breach Notification Form FAC-001
- Delay of Notification Form FAC-002

The purpose of notifying individuals of such incidents is to enable them to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm. To ensure giving timely and helpful notice to affected individuals, the following practices are required by Kentucky's data breach legislation:

Contents of Notification

1. To the extent possible, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired;

2. Contact information for the notifying agency, including the address, telephone number, and toll-free number if a toll-free number is maintained;

3. A description of the general acts of the agency, excluding disclosure of defenses used for the protection of information, to protect the personal information from further security breach; and

4. The toll-free numbers, addresses, and Web site addresses, along with a statement that the individual can obtain information from the following sources about steps the individual may take to avoid identity theft, for:
    - The major consumer credit reporting agencies;
    - The Federal Trade Commission; and
    - The Office of the Kentucky Attorney General.

Timing of Notification

- According to the data breach legislation passed in 2014 and that went into effect January 1st, 2015, each agency and public school has a total of 35 days from the time of their formal notification of agency contacts to "notify all individuals impacted by the security breach." Details about the type of notification, which can impact the cost, can be found in the legislation.

Contact Law Enforcement

- If your assessment leads you to reasonably believe that an unauthorized person through criminal activity versus by accident acquired restricted personal information, then a notification to law enforcement, such that would begin an investigation, should occur as well. This is over and above the notification required by KRS 61.931, ET SEQ. (HB 5).

Cost Considerations When Implementing Personal Data Security

Please note that none of the other states and private organizations identify the total cost to fully implement all three major areas mentioned above. But if cost was mentioned, it was a cap amount that had to be spent in notifying people of a potential compromise of their personal data. A cap is something that should be considered by the department and school districts.

KDE and every public school district will need to weigh the risk of a data security breach versus the cost to implement these recommendations. Some of the suggested items listed under Protection and Prevention can be very expensive to implement (e.g., encryption, intrusion detection systems), so some owners of data systems will implement these, and others will take their chances and will do the best they can with the methods they are now using. This will cause the costs to fully implement all the recommendations mentioned above to fluctuate greatly between all the different paper and electronic data systems in school districts and KDE. This makes it very difficult to estimate overall cost to implement statewide at this time. It is, however, fair to ask each organization to prepare for and implement these three major areas the best they can, while at the same time placing a cap on what must be spent toward actual notification.

Additional Resources

April 23, 2015 HB5 Kentucky K-12 Data Breach Webcast Archive - Direct link

April 23, 2015 HB5 Kentucky K-12 Data Breach Webcast Archive - Short link

Additional Commonwealth Office of Technology Resources

COT has the following enterprise policies in place that may assist meeting requirements for KRS 61.931, et seq. (HB 5) for "Reasonable security and breach investigation procedures and practices…" Districts are encouraged to review these documents and use them as examples, but customization will be required. These documents are written for COT and agencies in the Executive Cabinet of state government. Several of the processes within, such as contacting the Commonwealth Service Desk after an incident, will not be applicable for school districts.

- CIO-090 - Information Security Incident Response Policy
  Identifies the necessity and procedures for agencies and COT to identify and notify appropriate personnel when a security incident occurs.
- CIO-091 - Enterprise Information Security Program
  Aligns the Commonwealth's Enterprise Information Security Program with the security framework of the current National Institute of Security Standards (NIST) Special Publication 800-53.
- CIO-092 - Media Protection Policy
  Ensures proper provisions are in place to protect information stored on media, both

digital and non-digital, throughout the media's useful life until its sanitization or destruction.

Data Security Measures Already in Place For KDE and Public School Districts

- Anti-Virus/Malware/Spam/Spyware Protection
- Vulnerability Scanning
- System Patch Management
- Cloud/Offsite Resources
- Active Directory/Group Policy Objects
- Private IP implementation
- Distributed Denial of Service (DDOS) Mitigation
- Web Filtration
- Centrally Managed Firewalls
- Virtual Private Network Support
- Secure File Transfer
- Statewide Product Standards

KDE and district data housed physically in Frankfort are also protected by physical security

- Code Entry Systems to General Building (Logging System)
- Staffed Reception Area
- Visitor Sign In/Out
- Isolated Code Entry for Data Rooms (limited access)
- Monitor lock down systems (CYBEX)
- Power UPS Backup System
- Locked Rack Systems
- Closed Circuit Television Video Surveillance System with Video Capture at 15 Fountain Place and 14th floor, Capital Plaza Tower.
- Entry Intrusion Alarm Systems
- Systems located at the COT data facility take advantage of 24 hour security and authorized, escorted entry only