

Boone County Schools  
Data Security and Privacy  
2023 - 2024



## **Purpose**

Basic awareness of data security and privacy best practices. Notification to the Boone 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 credentials
- Loss/Theft of device
- Phishing
- Malware
- Application vulnerabilities
- Hackers
- Too Many Permissions
- Insider error

## **Current Boone County Measures to Prevent a Breach Include**

- 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/Closets/Cabinets
- 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
- Training/Communications for all district employees via email, Administrator Meetings, School Technology Coordinator 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)
- Mandatory password changes (complex) for all staff twice per school year
- Multi Factor Authentication
- 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 Boone County Schools.

# Appendix A

**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 noneducational 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.

**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.

### **61.931 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.

**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)."

## **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.)