
HOPKINS COUNTY SCHOOLS TECHNOLOGY DEPARTMENT



Data Security & Privacy

Prepared for: Hopkins County Board of Education

July 30, 2019



SUMMARY

702 KAR 1:170 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. This presentation on data security and privacy completes the requirement.

Objectives

- Provide basic awareness of data security and privacy best practices
- Notification to the Hopkins County Board of Education that the district has reviewed and implemented best practices

Relevant Board Policies & Procedures

- 01.61 – Records Management
- 01.61 AP.11 – Notice of Security Breach
- 09.14 – Student Records

Data Security Implementation Plan

- Identify and document data (both electronic and hardcopy) that need to be protected
- Audit current access to data by various groups of people and make adjustments as needed
- Document data security measures and security breach procedures
- Provide awareness training with all staff who have access to confidential data

Main Causes of Data Breaches

- Human Error
 - Accidental sharing (email, website, paper, etc.)
 - Weak or stolen passwords
 - Loss or theft of employee device (USB drive, laptop, etc.)
 - Phishing, clickbait
 - Everything Else
-

-
- Application vulnerabilities-unpatched software
 - Hackers
 - Malware & Ransomware

Security Breach Notification

Notify all individuals and agencies as outlined in KRS 61.933 if PII has been disclosed and will result in the likelihood of harm to one or more persons

One of these

- First name or first initial and last name
- Personal mark **AND**
- Unique biometric print/image

One or more of these

- Account number with PIN that would allow access to the account
- Social Security Number
- Taxpayer ID number
- Driver's license number or other ID number issued by any agency (student ID number)
- Passport number or other number issued by the US
- Individually identifiable health information except for education records covered by FERPA

Current Measures to Prevent a Breach

- Anti-Virus/Malware/Spam/Spyware Protection
 - Virtual Private Network Support
 - Secure File Transfer & Encryption
 - Statewide Product Standards
 - Locked Data Center
 - Locked File Cabinets/Doors
 - Limited Access (Need to Know)
 - Removal/Disabling of user accounts for staff no longer employed
-

-
- Staff confidentiality training
 - Vulnerability Scanning
 - System Patch Management
 - Cloud/Offsite Resources and Backups
 - Active Directory/Group Policy Object Management
 - Private IP implementation
 - Distributed Denial of Service (DDOS) Mitigation
 - Web Filtration
 - Centrally Managed Firewalls
 - Restricted Local Workstation Admins
 - Microsoft LAPS for Administrator account password management
-

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.)

Data Security and Breach Notification Best Practice Guide

Data Security and Breach Notification Best Practice Guide

Kentucky Department of Education (KDE)

V2.2 September 2015



- Legislation requires KDE to create and update this guide
- Available for download [here](#)

01.61 AP.11

POWERS AND DUTIES OF THE BOARD OF EDUCATION

01.61 AP.11

Notice of Security Breach & Investigation Procedures

PROTECTION AND PREVENTION

The District will take reasonable security measures in accordance with KRS 61.931 - KRS 61.933, to guard against the foreseeable loss or exposure of personal information that it maintains or possesses.

“Personal information” is defined as an individual’s first and last name or first initial and last name; personal mark; or unique biometric or genetic print or image, along with any data element listed below:

- Account number, credit or debit card number, that, in combination with any required security code, access code, or password would permit access to an account;
 - Social Security number;
-

-
- Taxpayer identification number that incorporates a Social Security number;
 - Driver's license number, state identification card number, or other individual identification number issued by any agency;
 - Passport number or other identification number issued by the United States government; or
 - 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.

Personal information does not include information that is lawfully made available to the general public pursuant to state or federal law or regulation.

A "security breach" refers to:

- an unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or is reasonably believed to compromise the security, confidentiality, or integrity of personal information and results in the likelihood of harm to one (1) or more individuals; or
- an 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 is reasonably believed to compromise the security, confidentiality, or integrity of personal information and results in the likelihood of harm to one (1) or more individuals.
- A 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 disclosed to others without authorization.

INITIAL ASSESSMENT/INVESTIGATION OF SECURITY INCIDENT AND NOTICE

When the District receives information or notice prompting a reasonable belief that an event compromising the security of personal information maintained by the District or nonaffiliated third party on behalf of the District may have occurred, the District shall conduct a reasonable initial assessment or investigation to determine whether the event constitutes a "security breach" under the above definition.

Notice of Security Breach & Investigation Procedures

INITIAL ASSESSMENT/INVESTIGATION OF SECURITY INCIDENT AND NOTICE (CONTINUED)

Once it is determined that a security breach relating to personal information has occurred, the District shall within seventy-two (72) hours: 1) notify the Commissioner of the Kentucky State Police, the Auditor of Public Accounts, the Kentucky Attorney General and the Education Commissioner and 2) begin a reasonable and prompt investigation to determine whether the security breach has resulted or is likely to result in the misuse of personal information.

FOLLOW-UP INVESTIGATION/ASSESSMENT IF SECURITY BREACH CONFIRMED

If it is determined after initial investigation that a security breach has occurred, the District shall complete an investigation and assessment of the incident to determine whether the security breach has resulted or is likely to result in the misuse of personal information, which may include the following:

- Depending on the nature of the breach and sensitivity of information, take reasonable near-term steps to mitigate further unauthorized disclosure of personal information and risk of harm.
- Consider designating a lead investigator and investigative team with expertise keyed to the event (e.g. utilization of available District IT professionals if breach involves electronically maintained information, internet, or web resources).
- Interview relevant individuals to learn about the circumstances surrounding the incident and review logs, tapes or other resources.
- Identify individual(s) affected by the breach.
- Determine what personal information has been compromised and how disclosed.
- If applicable, identify affected machines, devices, and IT resources and preserve backups, images and hardware where possible.
- Estimate the likely impact of the compromised data's exposure.
- Utilize professional assistance and consultation as necessary, analyze the likely cause of the breach.
- Coordinate internal and external communications related to the incident. Emphasize maintaining confidentiality during investigative stages of response activities.
- Seek involvement of law enforcement if there is reason to believe criminal activity has occurred.

Notice of Security Breach & Investigation Procedures

NOTIFICATION

Upon conclusion of the investigation, if it is determined that a security breach has occurred and that misuse of personal information has occurred or is likely to occur, the District shall within forty-eight (48) hours notify the Commissioner of the Kentucky State Police, the Auditor of Public Accounts, the Attorney General, the Commissioner of Education, and the Commissioner of the Department of Libraries and Archives. Within thirty-five (35) days of providing these notices, the District shall notify all individuals impacted by the security breach as provided by law.¹

These notices shall be delayed upon written request of a law enforcement agency that the notices would impede an investigation. Security Breach Forms are located on the Kentucky Finance & Administration Cabinet website:

<http://finance.ky.gov/SERVICES/FORMS/Pages/default.aspx>.

If the investigation determines that misuse of personal information has not occurred or is not likely to occur, the above agency contacts shall be provided notice of the determination. In this case, notice to affected individuals is not required, but the District should maintain records reflecting and supporting the determination.

CONTRACTS WITH NONAFFILIATED THIRD PARTIES - INFORMATION SECURITY

On or after January 1, 2015, agreements calling for the disclosure of “personal information” to nonaffiliated third parties shall require the third party contracting with the District to follow information breach and security standards at least as stringent as those applicable to the District.

Contracts with such third parties shall specify how costs of data breach investigations and notices are to be apportioned.

OTHER PRIVATE INFORMATION

In the case of breach of information made private by law that does not fall within the definition of “personal information”, the District may engage in similar investigative, response, or notification activities as provided above. Alternatively, the District may, after reasonable investigation, provide notice to the individual whose restricted personal information has been acquired by an unauthorized person. Notification will be made in the most expedient time frame possible and without unreasonable delay, except when a law enforcement agency advises the District that notification will impede criminal investigation. Notification should be provided to the individual within three (3) working days of discovery of the breach but no later than thirty (30) working days.

Depending on the number of people to be contacted, notification may be in the form of a face-to-face meeting, phone call, posting on a Web site or sending a written notice to each affected person’s home. Notice should include the specific information involved and, when known, an estimate of how long it has been exposed, to whom the information has been released and how the breach occurred. In addition, the individual should be advised whether the information remains in the physical possession of an unauthorized person, if it has been downloaded or copied, and/or, if known, whether it was used by an unauthorized person for identify theft or fraud purposes.

Notice of Security Breach & Investigation Procedures

REFERENCES:

¹KRS 61.933

KRS 61.931; KRS 61.932

702 KAR 001:170

Data Security and Breach Notification Best Practice Guide

Review/Revised: 7/30/2016
