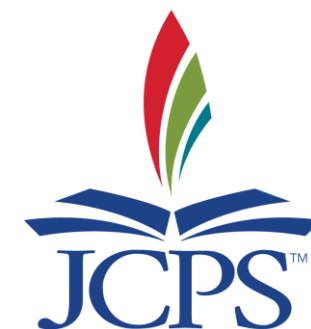




---

# Data Security & Privacy

Jefferson County Board of Education





---

# Purpose

- Basic awareness of data security and privacy best practices
- Notification to the local board that the district has reviewed and implemented best practices



---

# Current & Relevant Legislation

- Federal
  - FERPA (1974) – Family Educational Rights and Privacy Act
  - COPPA (1998) – Children’s Online Privacy Protection Act
  - CIPA (2000) – Children’s Internet Protection Act
  - Others – IDEA, PPRA, etc.
- State
  - Kentucky FERPA (1994 – KRS 160.700 et seq.)
  - HB 232 (signed into law April 10, 2014)
  - HB 5 (signed into law April 10, 2014; effective January 1, 2015)
  - 702 KAR 1:170 (filed with LRC August 13, 2015)



---

# House Bill 232

- Called for the creation of KRS 365.734
- 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 statute



---

# House Bill 5


- Called for the creation of KRS 61.931, 61.932, and 61.933
- Defines “Personal Information” (different from FERPA’s definition of personally identifiable 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

- Authorized by House Bills 5 and 232
- 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



---

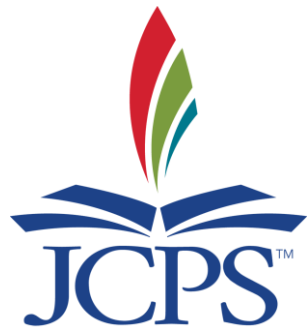
# Data Security and Breach Notification Best Practice Guide

## Data Security and Breach Notification Best Practice Guide

---

**Kentucky Department of Education (KDE)**

V2.2 September 2015





---

# Data Security Implementation Plan

- Data Classification
- Risk Assessment
- Policies and Procedures
- Security Awareness Training





---

# Main Causes of Data Breach

- Human Error
  - Accidental sharing (email, website, paper, etc.)
  - Weak or stolen passwords
  - Loss or theft of employee device (USB drive, laptop...)
  - Spear Phishing, clickbait
  - Social engineering
- Everything Else
  - Application vulnerabilities – unpatched software
  - Hackers
  - Malware



---

# Confidential Data

- Student education records except “directory” information in certain circumstances
- PII as defined by FERPA and House Bill 5



# 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		One or more of these	
<ul style="list-style-type: none"><li>• First name or first initial and last name</li><li>• Personal mark</li><li>• Unique biometric print/image</li></ul>	AND	<ul style="list-style-type: none"><li>• Account number with PIN that would allow access to the account</li><li>• Social Security Number</li><li>• Taxpayer ID number</li><li>• Driver's license number or other ID number issued by any agency (student ID number)</li><li>• Passport number or other number issued by the US</li><li>• Individually identifiable health information except for education records covered by FERPA</li></ul>	



---

# Student Data

- "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, email address, email messages, postal address, phone number, and any documents, photos, or unique identifiers relating to the student. (KRS 365.734)



---

# Cloud Providers

- KRS 365.734 prohibits cloud providers from processing student data for any purpose other than improving its services. Specifically prohibits the use of data for advertising and selling of student data.