

# Data Security, & Privacy

Livingston County Schools Presentation August 2017



# Purpose

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

# Current & 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
  - IDEA (2004) - Individuals with Disabilities Education Act
  - ESSA (2015) – Every Student Succeeds Act
  - Others –PPRA - Protection of Pupil Rights Act, 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)

# Relevant Board Policies & Procedures

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

# House Bill 232

- Called for the creation of KRS 365.734
- Prohibits the 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

- 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

- 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



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





# 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 (ie., password1)
  - Loss or theft of employee device (USB drive aka flash drive, laptop...)
- Phishing, clickbait
- 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

- 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 (KET/KDE)
- Vulnerability Scanning
- System Patch Management
- Cloud/Offsite Resources
- Active Directory/Group Policy Objects
- Private IP implementation (via Active Directory/DHCP)
- Distributed Denial of Service (DDOS) Mitigation
- Web Filtration (Lightspeed and enhanced firewalls)
- Centrally Managed Firewalls
- Virtual Private Network Support
- Secure File Transfer
- Statewide Product Standards
- Locked Data Center
- Locked File Cabinets/Doors
- Limited Access (Need to Know)
- Security settings on all workstations and servers
- Alert email notifications (DTC) for critical systems
- Removal of user accounts for staff no longer employed
- Staff confidentiality training
- Staff awareness digital security training via cloud based platform (currently KnowBe4)



# 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)



# What Can I Do?

- Always secure your workstation\device
- Keep a strong password: Between 8-15 case sensitive characters with a minimum of one numeral and one capital letter-no spaces. Passwords are prompted to change every 90 days
- NEVER use the same password for multiple services
- Use good practices when emailing (Confidential email should be flagged w/send and delivery receipt requests) Only email to the “need to know” personnel
- Use safe practices when browsing the Internet
- Report possible viruses immediately to the technology department
- Realize that “WE ARE ALL TARGETS” (Schools have valuable data)
- Make cyber & physical security a regular point of conversation (Although they are different, they are ever changing)



# Cloud Providers

- KRS 365.734 prohibits cloud providers from processing student data for any purpose other than improving its services. Specifically prohibits use of data for advertising and selling of student data.
- Current cloud providers/programs: Infinite Campus, Google (Classroom and Google Docs), Microsoft (Office365-One Drive), eProve Diagnostics from Advanced Ed, Lexia, Odysseyware, AIMS Web, WIDA, Follett Destiny (Library), Career Cruising (ILP's), KET Encyclomedia, MobyMax, Reading Plus, Renaissance Learning (Accelerated Reading, Math and Star), Study Island, Khan Academy, Prezi, Mosaic (food services), Certiport (CTE), Apex Learning ...

# Questions?

**Please contact me, if I don't know the answer, I will research to find resolution.**

**BJ (Rushing) Fern, District Technology Coordinator/Network Admin  
LCS District Technology Office  
c/o LCHS 750 US Hwy 60 W  
Smithland, KY 42081**

**Email: [bj.rushingfern@livingston.kyschools.us](mailto:bj.rushingfern@livingston.kyschools.us)**

**Office Phone: 270.928.2659 Office Fax: 270.928.2454  
Cell: 270.508.1193**

