Data Security & Privacy

August 21, 2017 Henderson County Board of Education Briefing

Purpose

- Basic awareness of data security and privacy best practices
- Notification to the local board that the district has reviewed and implemented best practices by 8/31 each year.

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
  - 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)

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

- 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

http://education.ky.gov/districts/tech/Documents/Data%20Security%20and%20Breach%20Notification%20Best%20Practice%20Guide.doc

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…)
  - Phishing, clickbait
- Everything Else
  - Application vulnerabilities – unpatched software
  - Hackers
  - Malware

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 and require annual awareness training with all staff who have access to confidential data
- Assign Data Stewards

Data Security Implementation Plan Cont.

- Require complex passwords for staff.
- Require password changes every 120 days.
- Enforcement of remote access authorization lists.
- Constant monitoring of data access, threat management, and user training.

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
- Unique biometric print/image

AND

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
- 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 Control
- Secure File Transfer
- Statewide Product Standards
- Locked Data Center/Access Control
- Locked File Cabinets/Doors
- Limited Access (Need to Know)
- Removal of user accounts for staff no longer employed
- Staff confidentiality training and planned security training

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 that improving its services. Specifically prohibits use of data for advertising and selling of student data.
- Current cloud providers/programs: Infinite Campus, Pearson (CIITS and others), NWEA (MAP), Google, Microsoft, Odysseyware, AIMS Web, WIN Learning, Career Cruising, KET Encyclomedia, Edmodo, Raz-Kids, Reading Plus, Study Island, Remind, IXL, Khan Academy,, and others…

Our Process

- If there is a suspected or potential breach employee must notify their immediate supervisor and Tech Dept. with 24 hours.
- Tech Dept. will investigate and determine if a breach has occurred.
- If yes, follow protocol outlined by KDE reporting to proper agencies.

Questions?