Data Security & Privacy

August 21, 2023 Henderson County Board of Education Briefing

Kris Gordon - HCS Technology Director

702 KAR 1:170

- “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.”

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 5 (2015 - KRS 61.931 et seq.)
  - HB 232 (2015 - KRS 365.732, KRS 365.734)
  - 702 KAR 1:170 (School district data security and breach procedures)

“House Bill 5”

- KRS 61.931, 61.932, 61.933, and 61.934 (2015)
- Generally requires that all Kentucky public agencies and their contracted vendors must implement, maintain, and update security procedures and practices, including taking any appropriate corrective action to safeguard against security breaches.
- Defines, for Kentucky, “Personal Information”
- Requires notification of specific state agencies and victims of a data breach.
- Outlines security breach notification procedures and timelines

“House Bill 232”

- KRS 365.732 and 365.734 (2015)
- Requires cloud computing service providers contracting with educational institutions to maintain security of student data and imposes limits what a cloud service provider can do with student data.
- Defines student data as including “the student’s name, email address, email messages, postal address, phone number, and any documents, photos, or unique identifiers relating to the student.”

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, NWEA (MAP), Google, Microsoft, Edgenuity, Raz-Kids, Reading Plus, Study Island, IXL, Khan Academy, Headsprout, Lexia, Renaissance and others…

KDE Data Security Best Practice Guidelines

https://education.ky.gov/districts/tech/Pages/Best-Practice.aspx

Security Breach Notification Requirements

In the event of a confirmed data breach we are required to 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.

Personally Identifiable Information includes:

One of these		One or more of these
• First name or first initial and last name • Personal mark • Unique biometric print/image	**AND**	• 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

Our Process

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

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

Henderson Co. Data Security Implementation

- We limit access to data and make adjustments as needed.
- We document data security measures and security breach procedures.
- We provide and require annual awareness training with all staff who have access to confidential data
- We require complex passwords for staff.

Data Security Implementation Plan Cont.

- We require password changes multiple times per year.
- We maintain a strict process of providing remote access.
- We constantly monitor data access, threat management, and provide user training.
- We require multi-factor authentication (MFA) for all staff accounts

Current Measures to Prevent a Breach

- Vulnerability Scanning
- System Patch Management
- Secure Cloud/Offsite Resources
- Private IP implementation
- Web Filtration
- Centrally Managed Firewalls
- Virtual Private Network (VPN)
- Secure File Transfer (SFTP)
- Locked File Cabinets/Doors
- External email banner
- Friendly Phishing campaigns
- Block all international logins
- Anti-Virus/Malware/Spam/Spyware Protection
- Active Directory/Group Policy Objects
- Distributed Denial of Service (DDOS) Mitigation
- Staff confidentiality and security training
- Deletion of accounts for staff no longer employed
- Limited data access (need to know basis)
- Locked Data Center/Access Control
- Email encryption
- Security audits
- Domestic Offsite Data backups