WVISD Data Security and Privacy
2023-2024
Walton-Verona Independent Schools
Walton, Kentucky

http://wv.kyschools.us

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 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.)

Source: http://education.ky.gov/districts/tech/pages/datacollection.aspx
"*The Family Education Rights and Privacy Act (FERPA) limits disclosure of personally identifiable data except under certain conditions. KDE limits access to identifiable data but does promote use of aggregated data for analysis and research. Public data is available through the Open House site.*

FERPA gives parents certain rights with respect to their children's education records. A school must provide a parent with an opportunity to inspect and review his or her child's education records within 45 days following its receipt of a request. Contact the school your child attends for more information on how to review his/her education records."

House Bill 232 (signed into law April 10, 2014)

Source: http://www.lrc.ky.gov/record/14rs/hb232.htm
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 (signed into law April 10, 2014; effective January 1, 2015)

Source: http://www.lrc.ky.gov/record/14rs/hb5.htm
Called for the creation of KRS 61.931, 61.932, and 61.933
Defines "Personal Information" or "PII" (different from FERPA's definition).
Requires school districts to establish "reasonable security and breach investigation procedures and practices".
Outlines security breach notification procedures and timelines.

702 KAR 1:170 (filed with LRC August 13, 2015)

Source: http://www.lrc.state.ky.us/kar/702/001/170.htm
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 Privacy Resources

Privacy Technical Assistance Center (PTAC)
Education Privacy Information Center
Data Quality Campaign
Fordham Center on Law and Information Policy
Kentucky Department for Libraries and Archives (Public School District Retention Schedule)

Data Security and Breach Notification Best Practice Guide

House Bill 341
Source: http://education.ky.gov/districts/tech/pages/best-practice.aspx
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

1. Accidental sharing (email, website, paper)
2. Weak or stolen passwords
3. Loss or theft of employee device
4. Phishing, clickbait
5. Application vulnerabilities
6. Hackers
7. Malware

Current Measures to Prevent a Breach

1. Reducing authentication providers
2. Staff password changes during school year
3. Require stronger passphrases for staff
4. Anti-Virus/Malware/Spam/Spyware Protection
5. Vulnerability Scanning
6. System Patch Management
7. Cloud/Offsite Resources
8. Active Directory/Group Policy Objects
9. Private IP implementation
10. Distributed Denial of Service (DDOS) Mitigation
11. Web Filtration
12. Centrally Managed Firewalls
13. Virtual Private Network Support
14. Secure File Transfer
15. Statewide Product Standards
16. Locked Data Center
17. Locked File Cabinets/Doors
18. BitLocker on staff devices
19. Multi-factor authentication
20. Geo-blocking data access to North America
21. Limited Access (Need to Know)
22. Removal of user accounts for staff no longer employed
23. Staff confidentiality training and planned security training
24. Promoting with staff to collect less data and/or only what is needed
25. Random security audits for software, services and apps
26. Coalition Insurance Solutions Cyber Policy
27. Device screen time outs, account time outs, and limited permissions

Summary

We have continued to enforce the policies and procedures set last year. We continue to review and enforce those policies when reviewing or purchasing new systems or software. It is our intent to continue due diligence in protecting data that relates to staff, students and the business of the WVISD.