

**WOODFORD COUNTY BOARD OF EDUCATION
AGENDA ITEM**

ITEM #: **DATE:** July 12, 2024

TOPIC/TITLE: Annual Data Security Update

PRESENTER: Josh Rayburn

ORIGIN:

- TOPIC PRESENTED FOR INFORMATION ONLY (No board action required.)
- ACTION REQUESTED AT THIS MEETING
- ITEM IS ON THE CONSENT AGENDA FOR APPROVAL
- ACTION REQUESTED AT FUTURE MEETING: (DATE)
- BOARD REVIEW REQUIRED BY
 - STATE OR FEDERAL LAW OR REGULATION
 - BOARD OF EDUCATION POLICY
 - OTHER:

PREVIOUS REVIEW, DISCUSSION OR ACTION:

- NO PREVIOUS BOARD REVIEW, DISCUSSION OR ACTION
- PREVIOUS REVIEW OR ACTION
 - DATE: July 24, 2023
 - ACTION:

BACKGROUND INFORMATION:

HB 5 requires an annual review of the data security protections and procedures.

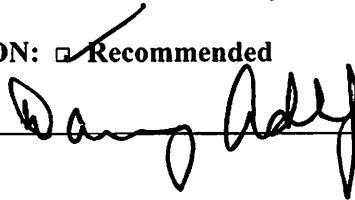
SUMMARY OF MAJOR ELEMENTS:

WCPS Board of Education acknowledges it has reviewed the Data Security and Breach Notifications Best Practice Guide (KDE) and implements practices to protect personal information within its systems.

IMPACT ON RESOURCES: No impact

TIMETABLE FOR FURTHER REVIEW OR ACTION: Review again by next August

SUPERINTENDENT'S RECOMMENDATION: Recommended Not Recommended





WOODFORD COUNTY PUBLIC SCHOOLS

330 Pisgah Pike • Versailles, Kentucky 40383-9214 • (859) 879-4600

Danny Adkins, Superintendent



July 12, 2024

Board Members,

We live in a connected world which has increased the need for digital data security in order to protect individuals' information. This led the Kentucky General Assembly to pass HB 232 (protection of student data by cloud vendors) and HB 5 (defines personally identifiable information and the procedures for security breach investigations/notifications) in April 2014. Together the laws require the district to annually acknowledge it has reviewed the Data Security and Breach Notification Best Practice Guide and implement practices to protect personal information. The technology department acknowledges that it has reviewed the guidance multiple times, taken steps to inform district employees of data security procedures, and worked to ensure our systems are protected. No network/system is 100% safe from being compromised but we are working hard to keep any data from being accessed by those without a "need to know."

Current actions are taken to protect personal information and prevent a breach.

- Safe Schools Training related to email and messaging
- Anti-Virus/Malware/Spam/Spyware Protection
- Private IP implementation
- Distributed Denial of Service (DDOS) Mitigation
- Implemented a 15-character phase requirement for device logon
- Web Filtering
- Centrally Managed Firewalls
- Fully Encrypted Virtual Private Network Support
- Secure File and Email Transfer
- Statewide Product Standards
- Locked Data Centers
- Disabling and Removal of user accounts and data for staff no longer employed, automated based on their end date in Munis.
- Disabling and Removal of student accounts and data for students who graduate or leave the district, automated based on their end date in Infinite Campus
- Data Security MOA for 3rd party vendors
- Hard drives destroyed on surplus workstations and servers
- Encourage all staff and students to keep Personal Identifiable Information (PII) off of local machines
- Provide data protection training for students through digital citizenship lessons promoting healthy online behaviors through the Library Media Service Teachers
- Syncing our Google and Microsoft accounts to further secure our network securities
- Implemented 2-factor Authentication for all staff-level access to our Google Workspace for Education. and Microsoft Office 365 infrastructures.
- Secured our Gmail system against spam, phishing, and malware by implementing the latest industry-standard email system protections.
- Subnet Isolation- All devices will be isolated to the current building they are in won't be able to communicate with another building on the network, thus creating a more secure environment.

BOARD MEMBERS

Angela McKale, Chair – Amanda Glass, Vice Chair
Adam Brickler – Sarah McCoun – Sherri Springate

Equal Education and Employment Opportunities

What happens when data breach is suspected?

- Notify several state agencies (attorney general, state police, etc.) within 72 hours
- 48 hours to notify agencies whether misuse of personal information has occurred or is likely to occur.
- Within 35 days notify all individuals impacted if a breach is confirmed.

Most common causes of data breaches

- Loss or theft of a USB Drive, Laptop, Tablet, or Smartphone with PII information on it
- Phishing attacks through email – someone asking you to give up PII
- Poor, shared, or stolen passwords
- Accidental sharing of PII through email, links, etc.

Feel free to contact me if you have further questions on this topic.

Sincerely,



Dr. Josh Rayburn
Chief Information Officer
Woodford County Public Schools

