

**WOODFORD COUNTY BOARD OF EDUCATION
AGENDA ITEM**

ITEM #: YUE **DATE:** July 19, 2019

TOPIC/TITLE: Annual Data Security Update

PRESENTER: Bob Gibson

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: August 27, 2018
 - ☐ 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 next August



SUPERINTENDENT'S RECOMMENDATION: ☐ Recommended ☐ Not Recommended



WOODFORD COUNTY PUBLIC SCHOOLS

7-17-19

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 (staff meetings in July/Aug/Sept) 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 taken to protect personal information and prevent a breach.

- Staff Data Security Meetings in all schools
- Anti-Virus/Malware/Spam/Spyware Protection
- Private IP implementation
- Distributed Denial of Service (DDOS) Mitigation
- 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
- Disabling and Removal of student accounts and data for students who graduate or leave district
- Data Security MOA for 3rd party vendors
- Hard drives destroyed on surplus workstations and servers
- Encourage all staff and students to keep PII out of cloud services and off of local machines
- Provide data protection training for students through the DDL program.

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.