



Data Security and Privacy

Annual Acknowledgement
SY 2026-2027

702 KAR 1:170

Requires that the district make the board aware prior to August 31 that it has reviewed KAR and reviewed & implemented actions found in the Data Security Breach Notification Best Practice Guide.



Data Security Procedures in Place

- Continuously audit current access to data by various groups and adjust as needed
 - Group Policies to reflect need for access
 - Secure File Transfer Protocol
 - CIO must approve programs prior to purchase to check for PII use
 - Preference to organizations that have signed the Student Privacy Pledge
- 
- A decorative horizontal bar at the bottom of the slide, consisting of a thick red line on top and a thinner black line on the bottom.

Data Security Procedures in Place

- Separate administrative accounts
 - Completed implementation of MFA on MUNIS accounts
 - Completed implementation of MFA on Microsoft Accounts
 - By the beginning of school year, we intend to have fully implemented Rapid Identity and in this school year, every staff member and student will have MFA procedures in place for accounts.
 - Microsoft Defender Deployment for Endpoint Protection
- 
- A thick horizontal bar at the bottom of the slide, consisting of a red upper section and a black lower section.

Data Security Procedures in Place

Train staff (extra training for those who have access to confidential data)

- Do not share passwords
- New password length and lifespan implemented as required by state
- Computer locking when inactive for set length of time
- Constant reminders to staff about phishing emails and data security
- Cybersecurity training for staff
- Browsing data deleted after a period of inactivity

Compliance with Student Safety

- Regular review of Smart Alerts in GoGuardian
 - All teachers have access to GoGuardian Teacher for supervision and management.
 - Continuously audit and update allowlists and blocklists
 - Automated emails are sent to Principals, Assistant Principals, and Counselors when a SmartAlert is received.
 - CIPA compliant base rules are in place for students in content filtering software.
- 
- A solid horizontal bar at the bottom of the slide, consisting of a thick red upper section and a thinner black lower section.

Maintain “open door” policy with staff to double check anything suspicious.

