To: Anchorage Independent Board of Education

From: Lee Collard, District Technology Coordinator

Date: July 22, 2024

Subject: Data Security Report

702 KAR 1:170, states that districts are required to acknowledge to the local board what is occurring to secure data. This is to be completed annually by August 31st.

During fiscal year **2023-24,** I and the CFO, Mr. Travis, have reviewed the legislative guidance put forth in HB 5 and 232 as well as best-practice suggestions offered from our cyber-insurance provider. We have shared appropriate and relevant information with staff and administrators, and will continue to comply with the legislative requirements and guidelines as they relate to business practice, software acquisitions, and access to and sharing of sensitive data. We will also continue to take advantage of data security and privacy training as needed and required.

The following information is offered as a summary of the type of data managed by different district and school positions.

Multi-Factor Authentication
In order to address the increasing frequency of cyber attacks faced by Kentucky schools, multi-factor-authentication (MFA) has been implemented across employee accounts for Microsoft365, Google, and Infinite Campus. The district financial system, MUNIS, similarly utilizes Tyler Identity Workforce (TID-W), which aligns the login credentials of the financial system with those of the KDE multi-factor-authentication requirements. Infinite Campus security has been significantly enhanced by switching to a unified login system. This system uses the same Windows MFA required by KDE for accessing school laptops and desktops.

Cafeteria Manager
The cafeteria manager has access to free- and reduced-lunch student information, payment checks, student numbers from Infinite Campus, family names, and addresses. To protect and secure data, paper reports are kept filed and behind a locked door, and digital records are coded and locked with a key known only to the cafeteria manager. Checks are placed in the safe and deposited daily, and items containing student identification numbers and mailing information are kept behind a locked door. Prints with sensitive information are shredded, and no confidential data is transferred via flash drives. The manager's door is always locked after hours, and she does not take sensitive information home. Electronic data is also protected by storing on the district server, not the local workstation.

School Nurse/Records Clerk
The school nurse/records clerk has access to paper and electronic health records, transcripts, and other data related to student enrollment. To protect and secure data, records are kept in locked file cabinets with limited access to other staff. Adhering to the Kentucky Archives and Records Commission retention schedule, and shredding items no longer needed, limits the risk of exposure from paper documents. Outside school hours and when she is away from her desk for a

prolonged period, the office door is locked and only the housekeepers and administrators have the key. No data is ever taken home or transported on flash drives, though when needed, transcripts may be delivered directly to receiving schools. Electronic data is also protected by storing on the district server, not the local workstation.

Infinite Campus Clerk/Food Services Director and District Office Secretary
The Infinite Campus Clerk/Food Services Director and District Office Secretary have access to personnel files, payroll information, social security numbers, the office safe, purchase orders, invoices, payment checks, academic records, student and family addresses and related information, tax billing information, and incoming faxes. To protect and secure data, personnel files are kept in a locked cabinet and behind a locked door; social security numbers are only kept with information requiring their use; deposits, bank cards, and stamps are stored in the safe; the office is locked at night with limited key access; no work travels home via flash drives or printouts; employment applications are kept in a locked cabinet; access to MUNIS data is restricted to purchase order information; and faxes are picked up and filed as they arrive. Electronic data is protected by storing on the district server, not the local workstation.

Technology Coordinator
The technology coordinator has access to all information stored on local servers and computers, and balance information within MUNIS technology accounts. To protect and secure data, the coordinator uses a local account when servicing computers and servers; has limited MUNIS access restricted to viewing only of technology accounts; processes surplus equipment through Bluegrass Recycling which provides certificates of destruction of all computers/laptops; configures new laptops with encrypted drives; and includes the latest Kentucky Department of Education supported antiviral and anti-malware software on all Windows computers. To further protect and secure data, the technology coordinator educates faculty and staff regarding types of information which are acceptable to send via email and which are not; attends trainings on data privacy and security, maintains a complex password change policy per KDE's guidance; and reminds data managers to only share what is needed when asked for information. In the rare occurrence of transferring data via a flash drive, the coordinator utilizes an encrypted drive attached to his keyring.

Finance Officer
The finance officer has access to both payroll and property tax records and their associated information, and unrestricted access to all data within MUNIS. He also has access to drivers' licenses, deposits, professional certificates, personnel files, and retirement and health information records. To protect and secure data, the finance officer stores all electronic files on the server instead of the local computer; keeps paper files in locked cabinets behind multiple locked doors with limited access; takes deposits directly to the bank (without detours), and neither travels with nor stores data on flash drives. The banking, retirement, and health information records he accesses are reached via secure portals. He is also vigilant with regard to the types of data which are acceptable or not to send via email.

This information will be reviewed annually.