Adair County School District
Data Management Policy

The Adair County School District's data must be managed, utilized, and protected in accordance with federal and state laws and school district policies to ensure its integrity, availability, and confidentiality. Each employee or agent of the Adair County School District that utilizes data for the purpose of performing his/her job duties or other functions directly related to his/her contractual affiliation with the Adair County School District is responsible for the proper handling of data resources under his/her control. Specifically,

- Each employee must protect the security and integrity of all data for which he/she is responsible for.
- Each employee must only access and utilize the data for which he/she is authorized to access for the purpose of performing his/her assigned job tasks.
- No data should be transferred or stored on personally owned computers or storage devices. All data must remain on district-owned network servers, computers, and resources.
- Each employee must safeguard their assigned username and password for district-level and web-based (Infinite Campus, etc.) applications to prevent unauthorized access by others.
- Each employee must realize that e-mail is not private and should refrain from sending confidential data via e-mail, which may inadvertently be sent or forwarded to the wrong person.
- Each employee will be assigned only the rights to data that pertain to his/her job function, as determined by district administration and/or job descriptions. Access to additional data will be provided as deemed necessary and must be requested in writing by the employee's immediate supervisor. The Superintendent or district-level designee will determine if additional rights to data may be assigned.
- Each employee must immediately report any suspected security breach or misuse of data to his/her building level administrator. The building level administrator must immediately notify the Superintendent or designee of the data compromise.

Types of data include: personnel records, performance evaluations, payroll records, school and district financial records, student and staff disciplinary records, student grades and attendance records, student and staff ID and/or social security numbers, free and reduced lunch records, student and staff health records, Internet usage and e-mail records, and any other data utilized within the district. Some types of data may have specific and additional policies for their management and utilization, which must also be followed.

Violations of this policy include, but are not limited to: accessing data of which the employee has no legitimate right; enabling unauthorized individuals to access data; disclosing data in a manner that violates district policies and procedures and/or federal or state regulations and/or laws; altering, damaging, or destroying data; inadequately protecting restricted data; or ignoring the requirements for the proper management, use, and protection of data resources. Violations may result in disciplinary and/or legal action that is pursuant to district policies and federal and state laws.