

TECHNOLOGY AND DATA SECURITY

The Riceville Community School District recognizes the increasingly vital role technology plays in society. It is the intent of the district to support secure data systems in the district, including security for all personally identifiable information (PII) that is stored digitally on district-maintained devices, computers and networks. The purpose of this policy is to ensure the secure use and handling of all district data, computer systems, devices and technology equipment by district students, employees, and data users.

The district may use of third-party vendors to perform necessary education functions for the district. Utilizing third party vendors to outsource functions the district would traditionally perform provides a cost-effective means to deliver high quality educational opportunities to all students. However, it is paramount that third party vendors with access to sensitive data and PII of district students, employees and data users be held to the highest standards of data privacy and security.

The selection of third-party vendors shall be in accordance with appropriate law and policy. Third-party vendors with access to PII shall meet all qualifications to be designated as a School Official under the Family Educational Rights and Privacy Act (FERPA). The superintendent or designee shall recommend to the Board that any approved contract with a third-party vendor will require that the vendor comply with all applicable state and federal laws, rules, or regulations, regarding the privacy of PII.

It is the responsibility of the superintendent to develop procedures for the district to enhance the security of data and the learning environment. The procedures shall address, but not be limited to, the following topics:

Access Control –Access control governs who may access what information within the district and the way users may access the information. It is the responsibility of the Superintendent **or** designee to determine which individuals will have access to district networks, devices and data; and to what extent such access will be granted. System and network access will be granted based upon a need-to-have requirement, with the least amount of access to data and programs by the user as possible.

Security Management –Security management addresses protections and security measures used to protect digital data. These include measures related to audits and remediation, as well as security plans for responding to, reporting and remediating security incidents. It is the responsibility of the superintendent or designee to develop procedures to govern the secure creation, storage and transmission of any sensitive data and personally identifiable information (PII). The Superintendent or designee shall implement appropriate controls to regulate data moving between trusted internal resources to external entities.

Technology and Data Use Training –Technology and data use training addresses acceptable use best practices to safeguard data for students, employees and staff. It is the responsibility of the Superintendent or designee to help ensure appropriate training on proper data and technology use.

Note: This policy and accompanying regulation are not mandatory for districts. This policy is intended as guidance for districts. Data and technology security are very broad topic areas, and the purpose of this policy is to attempt to break down this subject into more manageable topics for districts. In deciding how and when to implement data safeguards, districts should balance the already existing need to safeguard data with the resources they have available.

Legal References:

20 U.S.C. §1232g; 34 C.F.R. Part 99

47 U.S.C. §254

20 U.S.C. §6777

Iowa Code §§ 715C

Approved: September 19, 2022 Reviewed: November 17, 2025 Revised: July 13, 2026