



Policy EHA: Personal Data Privacy and Security

Status: DRAFT - Second Reading

Original Adopted Date: 01/16/2018 | **Last Reviewed Date:** 05/12/2026

The Wyoming Department of Education has released School District Data Security Guidelines to establish guidelines for school districts for the collection, access, privacy, security and use of student data by school districts. The District desires to generally implement and follow the guidelines as established by the Wyoming Department of Education and does hereby direct the School District Technology Director to implement procedures to carry out the recommendations set forth in the recommended School District Data Security Guidelines referenced in Wyoming Department of Education Memorandum No. 2017-105 released September 25, 2017.

The board recognizes the district's responsibility to collect, access, retain, secure, use, and dispose of personal data in a lawful and responsible manner. The district shall maintain policies, procedures, and practices governing personal data consistent with applicable law and the legitimate operational, educational, legal, and administrative needs of the district. For purposes of this policy, "personal data" means information that is linked or reasonably linkable to an identified or identifiable natural person or to a personal digital identity, as defined by law.

The school district shall not purchase, sell, trade or transfer personal data without the express written consent of the natural person whom the personal data references except as otherwise expressly provided by law. The district shall collect and maintain only the personal data reasonably necessary to carry out lawful district functions. The district shall identify and maintain the specific purposes for which categories of personal data are collected and retained. Personal data shall not be collected, retained, used, or disclosed except as authorized by law and for purposes reasonably related to the district's operations and legal obligations.

Access to personal data shall be limited to authorized employees, officials, agents, and service providers who have a legitimate educational, operational, administrative, legal, or safety-related need for access in order to perform assigned duties or provide contracted services. The district shall maintain reasonable administrative, technical, and physical safeguards to protect personal data against unauthorized access, acquisition, use, modification, disclosure, or destruction.

The district shall not retain personal data longer than reasonably necessary to fulfill the purpose for which it was collected, except as otherwise required by law or district records retention requirements. Personal data shall not be maintained for longer than three (3) years unless a longer retention period is required by law or is authorized by written district policy or administrative procedures identifying the extended retention period and a reasonable justification for that retention. Examples of laws which require longer retention periods for specific records are the Family Educational Rights and Privacy Act (FERPA) (20 USC 1232g) and its implementing regulations, Wyoming statutory records retention laws (W.S. 9-2-405 through 9-2-413), and the Wyoming records retention schedules adopted by the Wyoming State Archives and Historical Department.

A current or former Wyoming resident, or an authorized representative, may request access to personal data pertaining to that resident and may object to the accuracy, completeness, pertinence, timeliness, relevance, retention, dissemination, or denial of access to that data, as permitted by law. The district shall respond to qualifying requests and objections within the time required by law and other applicable district policies. If no specific timeline is required by an applicable law or policy, the district shall respond within 60 (sixty) days of the receipt of an objection. The district shall respond by providing the information required by W.S. 9-21-202(c).

The district may disclose personal data to nongovernmental entities only as authorized by law and only for purposes consistent with the district's lawful functions. Contracts with nongovernmental entities receiving personal data from the district shall require appropriate protection of that data and, when the data is no longer necessary for the contracted service, return or destruction of the data in accordance with law, contract terms, and district procedures.

The superintendent or designee shall develop and implement administrative procedures necessary to carry out this policy, including procedures addressing data classification, access controls, retention, destruction, security safeguards, breach or incident response, records requests, and vendor or contractor data protection. In implementing this policy, the superintendent or designee may rely on and coordinate this policy with other board policies and administrative procedures governing records, technology systems, student records, employee records, security, and records retention.

This policy shall be interpreted and applied in a manner consistent with applicable state and federal law, including laws governing student education records, employee records, public records, records retention, confidentiality, and

data security. To the extent another state or federal law imposes a more specific or controlling requirement, that law shall govern.

Nothing in this policy shall be construed to alter or modify or abrogate the rights, responsibilities, procedures, and duties with respect to student records as defined in other district policies governing student records.
