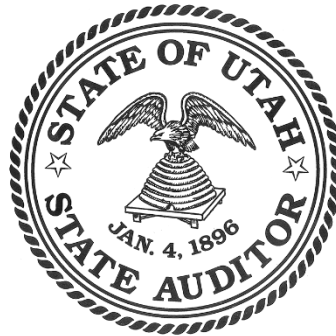


STATE OF UTAH
OFFICE OF THE UTAH STATE AUDITOR



TINA M. CANNON
UTAH STATE AUDITOR

Nebo School District

Privacy Audit Report

For the year ended December 31, 2025

Report No. PA-25-04

Office of the Utah State Auditor

Audit Leadership:

Tina M. Cannon, State Auditor

Warisara Watanawongworakula, CPA, CISA, Information Systems Audit Supervisor

Mark Meyer, CIPM, Assistant State Privacy Auditor

Tristan Olcott, Cybersecurity Specialist

Table of Contents

Management Letter No. PA-25-04 1

Findings & Recommendations 3

 Finding 1. Incident and Breach Methodology Not Fully Aligned with
 Requirements.....3

 Finding 2. Privacy Notices Not Fully Compliant.....4

 Finding 3. Annual Privacy Program Report Improvement Strategies Incomplete
 6

 Finding 4. Amendment and Correction Process Not Fully Aligned 6

Appendix A – Summary of Findings.....8





TINA M. CANNON
UTAH STATE AUDITOR

Management Letter No. PA-25-04

October 13, 2026

Nebo School Board, Audit Committee,
and
Rick Nielsen, Superintendent
Nebo School District
350 South Main
Spanish Fork, UT 84660

Dear Superintendent Nielsen,

As authorized under Utah Code §67-3-13(2)(f), the Office of the Utah State Auditor (OSA) conducted a privacy audit of Nebo School District (District). The objective of the audit was to assess the District's overall compliance with the Utah Government Data Privacy Act (GDPA), Utah Code §63-19, and other applicable privacy requirements. The audit evaluated the District's privacy program and related controls over the collection, use, retention, disposition, and sharing of personal data, as well as privacy governance, training, notices, contractor oversight, and incident and breach response.

The procedures of this audit do not constitute an audit conducted in accordance with generally accepted auditing standards, the objectives of which would be the expression of an opinion on the District's compliance with applicable privacy requirements. Accordingly, we do not express such an opinion.

Methodology

To accomplish the audit objective, we performed the following procedures:

1. Reviewed applicable laws, regulations, and guidance relevant to governmental and student data privacy;
2. Reviewed selected District policies, procedures, training materials, privacy notices, data collection forms, student-data documentation, vendor and application records, retention and disposition practices, data-sharing practices, and incident-response documentation;
3. Evaluated selected privacy-program controls and practices, including privacy governance and reporting, employee training, contract oversight, privacy notices, data minimization, data sharing, incident response, and required notifications; and

4. Interviewed selected District personnel to understand privacy responsibilities, data-handling practices, privacy-program implementation, and incident response.

Findings Overview

Our audit found that the District is not in full compliance with applicable state data privacy requirements. While a privacy program has been initiated, critical elements related to incident response, public disclosures, reporting, and student rights remain incomplete. The findings outline issues with the District's incident and breach methodology, privacy notices, annual privacy program report, and the student record amendment and correction process.

Our review was designed to assess the District's overall compliance with state privacy statutes and other applicable requirements. The audit did not examine every form, system, process, transaction, or record. We used certain documents, practices, and samples to evaluate the District's privacy program and related controls. Accordingly, our findings reflect the conditions identified through the procedures performed and may not include every instance of noncompliance or control weakness.

Why These Findings Matter

Local Education Agency (LEA) systems handle sensitive personal information about children. Mishandling or improper access to this data can result in reputational harm, privacy violations, identity theft, or other misuse of personal information. Without effective monitoring and safeguards, privacy incidents may go undetected or unaddressed, increasing the risk that sensitive data will be accessed, used, or disclosed without authorization.

We appreciate the courtesy and assistance District personnel extended to us during the course of this engagement, and we look forward to a continuing professional relationship.

Sincerely,

Tina Cannon
Utah State Auditor

cc: Cory Little, Technology Curriculum Specialist
Garrett Andersen, Technology Coordinator
Tim Beardall, Internal Auditor
Jeff Peterson, Associate Legal Counsel

Findings & Recommendations

Finding 1. Incident and Breach Methodology Not Fully Aligned with Requirements

The District's Incident Response Plan does not include the specific data breach notification requirements mandated by Utah law for government entities and school districts. The plan's "Notification Requirements" appendix (Appendix IV) primarily references external frameworks, such as HIPAA and GDPR, instead of the required state procedures. This omission creates a risk that the District will not follow proper notification timelines and channels during a data breach. Specifically, the plan does not clearly document notification procedures for the Utah Cyber Center, the Office of the Attorney General, affected individuals, or the Utah State Board of Education Superintendent for significant student-data breaches.

Breach reporting requirements under Utah statutes and administrative rules include the following:

- **Government Entity Reporting** (Utah Code § 63A-19-405): Mandatory reporting to the Utah Cyber Center and reporting to the Office of the Attorney General for qualifying breaches affecting 500 or more individuals.
- **Individual Notification** (Utah Code § 63A-19-406): Mandatory notification procedures for affected individuals following a breach.
- **Student Data Breaches** (Utah Admin. Rule R277-487-3(3)): Requirements for LEAs to report significant breaches of student data, whether experienced by the LEA or a third-party vendor, to the USBE Superintendent within 10 business days of initial discovery.

The process used to develop and review the District's Incident Response Plan did not identify and incorporate all statutory and regulatory notification requirements applicable to a Utah governmental education entity.

Without fully aligned procedures, District personnel lack clear, documented guidance regarding state and education specific reporting channels, notification triggers, timelines, and documentation requirements. This gap increases the risk of inconsistent, noncompliant, or untimely notification decisions during a reportable data breach.

Recommendation

We recommend that the District revise Appendix IV of the Incident Response Plan to retain other frameworks to the extent applicable and add a dedicated Utah-specific notification section. The revised section should clearly document the notification workflows, triggers, timelines, content requirements, responsible parties, and reporting procedures applicable to the Utah Cyber Center, the Office of the Attorney General, affected individuals, and the Utah State Board of Education Superintendent.

District's Corrective Action Plan

Nebo School District's technology and security officials are aware of the reporting requirements and have been in communication with the Cyber Center regarding notification procedures. Nebo is currently updating its Incident Response Plan to include all reporting requirements. The expected completion date is 10/15/2026.

Finding 2. Privacy Notices Not Fully Compliant

The privacy notices reviewed did not fully reflect the personal data collected or include all applicable statutory elements. We identified the following issues:

1. Student Data Collection Notice

The District's Student Data Collection Notice did not identify refugee background information collected through the Online Registration Form. The refugee-background field is part of the Utah State Board of Education's Home Language Survey used during student registration and is collected as part of the District's student language-identification process.

Utah Code §53E-9-305 requires an education entity's Student Data Collection Notice to state the student data the education entity collects. Furthermore, under Subsection (4) of the statute, an education entity is only authorized to collect student data if it has first provided a compliant notice. Because refugee background information is collected during registration but was omitted from the Student Data Collection Notice, the collection itself is not in compliance with statutory disclosure requirements, reducing transparency for families and placing the District in violation of the state's legal collection authority.

2. Collection-Point Privacy Notices

The Individualized Education Program Enrollment Form and Online Registration Form did not include or conspicuously link to a collection-specific privacy notice containing all elements identified in Utah Code §63A-19-402.

As stated in Utah Code §63A-19-402, a governmental entity must provide a privacy notice when requesting or collecting personal data. By omitting these notices on enrollment and registration forms, the District fails to inform individuals of their rights and the intended uses of their personal data at the precise moment it is collected.

3. Website Privacy Notice

The District's Website Privacy Notice did not include the following information required by Utah Code §63A-19-402.5:

- a clear method for users to request access to or correction of their personal data;
- instructions for filing a complaint with the data privacy ombudsperson;
- information regarding at-risk employee record classification;
- information about website tracking technologies; or
- the applicable record series.

The notice did successfully identify the District as the responsible governmental entity, provide contact information, describe the user data collected and its intended uses, and identify general classes of parties with whom the data may be shared.

However, because the required elements listed above were omitted, the public-facing notice does not fully disclose all statutorily mandated transparency disclosures. Specifically, the omission of these elements deprives website visitors of clear, publicly available instructions on how to submit inquiries to the District, how to file external complaints, and how at risk employees can request to protect their records.

Recommendation

We recommend that the District:

1. **Student Data Collection Notice**
Revise its Student Data Collection Notice to accurately identify the student data collected through the District's registration process, including refugee-background information collected as part of the USBE Home Language Survey.
2. **Collection-Point Privacy Notices**
Revise the applicable collection points to include or conspicuously link to privacy notices containing all applicable elements required by Utah Code §63A-19-402 and ensure the notices are provided through the required methods.
3. **Website Privacy Notice**
Revise its Website Privacy Notice to include all applicable elements required by Utah Code §63A-19-402.5, including the omitted information identified above.

District's Corrective Action Plan

The District is amending its Student Data Collection Notice to include refugee background information. Such information is collected from a very limited number of students as part of the home language survey required by USBE. The District is also linking its data privacy notice to the forms and the online registration process. Finally, the District's website privacy notice, which was last

updated in 2024 before the GDPR was enacted, is being updated to include the new statutory requirements. The expected completion date is 10/31/2026.

Finding 3. Annual Privacy Program Report Improvement Strategies Incomplete

The District's annual Privacy Program Report identifies a single improvement strategy concerning the annual review of data-sharing partners. However, the report omits critical disclosures regarding noncompliant, preexisting processing activities and fails to specify improvement strategies for other privacy program components that fell short of target maturity levels.

Utah Code §63A-19-401.3(1)(b)(ii) requires the annual Privacy Program Report to include a description of strategies for improving the governmental entity's privacy program and practices.

The District's report-development process did not ensure that specific improvement strategies were documented for all applicable privacy-program components identified for improvement. As a result, management and oversight bodies have limited information for monitoring planned improvements and progress toward the District's identified target maturity levels.

Recommendation

We recommend that the District ensure future Privacy Program Reports fully disclose all noncompliant, preexisting data-processing activities and establish measurable improvement strategies for all program components below target maturity levels.

District's Corrective Action Plan

The District's 2025 annual privacy report included some improvement strategies. The 2026 report is currently being prepared and will include additional improvement strategies for relevant areas. The expected completion date is 12/31/2026.

Finding 4. Amendment and Correction Process Not Fully Aligned

The District has a documented amendment and correction process; however, the Student Records and Data Protection Policy contains inconsistent provisions regarding the rights of eligible students. Section 4.2.2 recognizes that FERPA rights transfer from parents to eligible students under certain circumstances; however, Section 6 describes the applicable amendment, notice, and hearing procedures primarily in terms of parents without carrying that transfer of rights through to the detailed procedures. As a result, the two sections directly contradict each other: one establishes that eligible students hold the rights, while the other describes how those rights are exercised solely in terms of parents.

Utah Code §63A-19-403 requires a governmental entity that collects personal data to provide a procedure by which an individual, or the individual's legal guardian, may request amendment or correction of personal data. FERPA, including 34 CFR § 99.5 and 34 CFR Part 99, Subpart C, establishes amendment, notice, hearing, and statement rights for parents and eligible students.

The District's general transfer-of-rights provision in Section 4.2.2 was not carried through the detailed amendment and hearing procedures in Section 6. Consequently, eligible students and District personnel may be uncertain whether and how an eligible student may independently request amendment of an education record, receive notice of the District's decision, request a hearing when the District declines to amend the record, or place a statement in the record following an unfavorable decision. This ambiguity increases the risk that the procedures will not be understood or applied consistently.

Recommendation

We recommend that the District update the Student Records and Data Protection Policy, Section 6, to clearly explain how the applicable amendment, notice, hearing, and statement procedures apply to eligible students after FERPA rights have transferred.

District's Corrective Action Plan

The rights afforded to parents under NSD Policy JO have always been applied to eligible students as well. The transfer of rights paragraph means precisely that any right afforded to a parent in the policy also applies to an eligible student, as required by FERPA. Nevertheless, the policy is being reviewed to determine whether it could more clearly communicate that the amendment and correction rights also apply to eligible students. The expected completion date is 12/31/2026 if change is approved by the Nebo School District Board.

Appendix A – Summary of Findings

Finding #	Issues Identified	Statute	OSA's Recommendation	District's Corrective Action Plan	OSA Assessment
1	Incident and Breach Methodology Not Fully Aligned with Requirements	Utah Code §63A-19-405, 406; Utah Admin. Rule R277-487-3(3)	Revise Appendix IV of the Incident Response Plan to add a Utah-specific notification section documenting applicable workflows, triggers, timelines, content requirements, responsible parties, and reporting procedures for the Utah Cyber Center, Office of the Attorney General, affected individuals, and Utah State Board of Education Superintendent.	The District is fully aware of the reporting requirements and have been in communication with the Utah Cyber Center. We are currently updating our Incident Response Plan to explicitly incorporate all required state and education-specific procedures. Expected completion date is 10/15/2026.	Nebo School District has concurred with our findings and outlined corrective action plans that are currently underway. Because the final components of the District's Corrective Action Plan are scheduled for completion on December 31, 2026, the Office of the State Auditor will conduct a follow-up review during the first quarter of 2027, following full implementation, to evaluate compliance and the effectiveness of these revised policies
2	Privacy Notices Not Fully Compliant	Utah Code §63A-19-401, 402, 402.5; §53E-9-305	Update the Student Data Collection Notice to accurately reflect data collected; provide compliant notices at applicable collection points; and complete the Website Privacy Notice.	The District agrees to amend our Student Data Collection Notice to include the requested refugee background data element. The district is also actively linking our privacy notices directly to all data collection forms and updating our main website's privacy notice to comply with all new statutory requirements.	Refer to finding #1.

				Expected completion date is 10/31/2026.	
3	Annual Privacy Program Report Improvement Strategies Incomplete	Utah Code §63A-19-401.3	Revise the future Privacy Program Reports to fully disclose all noncompliant, preexisting data-processing activities and establish measurable improvement strategies for all program components below target maturity levels.	While the 2025 report did outline some improvement strategies, the District confirms that the 2026 report (currently in preparation) will include more comprehensive and detailed improvement strategies across all relevant compliance areas. Expected completion date is 12/31/2026.	Refer to finding #1.
4	Amendment and Correction Process Not Fully Aligned	Utah Code §63A-19-403; 34 CFR § 99.5 and Part 99, Subpart C	Update Section 6 of the Student Records and Data Protection Policy to clearly explain how amendment, notice, hearing, and statement procedures apply to eligible students after FERPA rights have transferred.	The amendment and correction rights afforded to parents have always been applied directly to eligible students in practice, as required by FERPA. However, the District acknowledges that the policy language could be clearer and are currently reviewing it to explicitly communicate this application to eligible students. Expected completion date is 12/31/2026 if the change is approved by the Nebo School District Board.	Refer to finding #1.