

Please see the information below as a follow up to the AOE's testimony from March 14, 2025.

- Support to the field regarding PowerSchool data breach:
 - The Agency sent out multiple communications (please see the email below) to share information and convened meetings to facilitate information sharing between districts. We continue to share information as we receive it.
- Projects ADS is working on for AOE:
 - Child Nutrition Management System
 - Educator Licensing System
 - Dual Enrollment Data System
 - Grants Management System – Contract Amendment and maintenance and support
 - School Based Electronic Health Records / IEP System
 - Azure Migration
 - Ed-Fi
 - Annual Snapshot (State Report Card)
 - Financial Database Support
 - Independent School Tuition Rate Setting Application
 - USDA Surplus Food Ordering Application
 - Home Study data collection
 - Home Language Survey
 - VTData Front End
 - Special Education CRM/Complaint Tracking System

Subject: Response to the PowerSchool Breach

Good afternoon, Superintendents.

I am reaching out about the recent cybersecurity breach involving PowerSchool, which may have impacted some Vermont districts. PowerSchool notified its subscribers yesterday about a national breach, and while not all Vermont PowerSchool subscribers are affected, we want to ensure that you have the information and support you need. Below is a notice sent to your education technology director/IT manager today, I know many of you have already been in contact with them to discuss the situation and its potential implications. The impact of this breach may vary from district to district. We strongly encourage any affected districts to reach out to VSBIT or your insurance provider immediately for further assistance and guidance.

The Vermont Attorney General's Office has published [security breach guidance](#) for businesses and organizations that may experience a breach. Within that publication are model letters for consideration of use. The template language

below should **not** be used by a Vermont SU/SD without first consulting their own legal team regarding the language and information in the message:

(School District Name) was notified (date) by our district's Student Information System (SIS) provider PowerSchool that on December 28, 2024 they became aware of a potential cybersecurity incident. An SIS is a software application specifically designed to manage student-related data in educational institutions. PowerSchool's incident involved unauthorized access to certain information through one of their community-focused customer support portals. Through this incident the unauthorized party gained access to certain PowerSchool SIS customer data using a compromised credential. PowerSchool is a global provider and manager of data for school districts and systems throughout the United States and globally.

(School District Name) was informed by PowerSchool that the district data stored in their system may have been compromised. We are working with PowerSchool to determine the breadth of this compromise. We will update the school community with more information as it becomes available.

We understand that this news may be concerning, but please be assured that the Agency takes incidents involving student information very seriously and is committed to ensuring that all necessary measures are in place to safeguard it.

The Agency's cybersecurity education technology staff member, Lisa Helme, has been in contact with the education technology directors/IT managers of subscribing PowerSchool districts about the incident. Your district staff leader in this area can inform you of the specific impact this incident will have on your SIS and student data. Lisa is available to assist districts as needed. She can be reached via email at lisa.helme@vermont.gov. Thank you for your attention to this matter and for your continued dedication to the safety and security of students and staff.

Sincerely,

Zoie Saunders, M.Ed.
Secretary of Education