An Idaho public charter school creating patriotic & educated leaders
Located in the Historic New Sweden Building 1736 S 35th W, Idaho Falls, Idaho

Subject: Important Notice: PowerSchool Data Breach

Dear Attorney General's Office,

We are writing to inform you of a data breach involving PowerSchool, the platform we use to manage student directories, course enrollments, report cards, attendance, and demographics. On December 28, 2024, PowerSchool discovered unauthorized access to its PowerSource service. It stores Student Information for over 60 million students and over 18,000 schools in more than 90 countries, including more than 90 of the top 100 districts by student enrollment in the United States.

The breach affects ALL schools that use PowerSchool and the compromised information includes the following types:

- Student names
- Student ID numbers
- Course enrollments/grades
- Student, Parent, and Staff Demographic information, including addresses, email addresses, and phone numbers

PowerSchool assures us that they have taken appropriate steps to prevent further unauthorized access or misuse of this data. Importantly, American Heritage does not collect financial information or Social Security numbers in PowerSchool, so we believe the compromised data is primarily limited to student/staff directory and course information.

We are attaching the information that was sent from PowerSchool about this incident. Please feel free to reach out to us if you have any questions or concerns.

Sincerely,

Dr. Tiffnee Hurst

Head Administrator

American Heritage Charter School

Dear Valued Customer,

As the Technical Contact for your district or school, we are reaching out to inform you that on December 28, 2024, PowerSchool become aware of a potential cybersecurity incident involving unauthorized access to certain information through one of our community-focused customer support portals, PowerSource. Over the succeeding days, our investigation determined that an unauthorized party gained access to certain PowerSchool Student Information System ("SIS") customer data using a compromised credential, and we regret to inform you that your data was accessed.

Please review the following information and be sure to share this with relevant security individuals at your organization.

As soon as we learned of the potential incident, we immediately engaged our cybersecurity response protocols and mobilized a cross-functional response team, including senior leadership and third-party cybersecurity experts. We have also informed law enforcement.

We can confirm that the information accessed belongs to certain SIS customers and relates to families and educators, including those from your organization. The unauthorized access point was isolated to our PowerSource portal. As the PowerSource portal only permits access to the SIS database, **we can confirm no other PowerSchool products were affected as a result of this incident**.

Importantly, the incident is contained, and we have no evidence of malware or continued unauthorized activity in the PowerSchool environment. PowerSchool is not experiencing, nor expects to experience, any operational disruption and continues to provide services as normal to our customers.

Rest assured, we have taken all appropriate steps to prevent the data involved from further unauthorized access or misuse. We do not anticipate the data being shared or made public, and we believe it has been deleted without any further replication or dissemination.

We have also deactivated the compromised credential and restricted all access to the affected portal. Lastly, we have conducted a full password reset and further tightened password and access control for all PowerSource customer support portal accounts.

PowerSchool is committed to working diligently with customers to communicate with your educators, families, and other stakeholders. We are equipped to conduct a thorough notification process to all impacted individuals. Over the coming weeks, we ask for your patience and collaboration as we work through the details of this notification process.

We have taken all appropriate steps to further prevent the exposure of information affected by this incident. While we are unaware of and do not expect any actual or attempted misuse of personal information or any financial harm to impacted individuals as a result of this incident, PowerSchool will be providing credit monitoring to affected adults and identity protection services to affected minors in accordance with regulatory and contractual obligations. The particular information compromised will vary by impacted customer. We anticipate that only a subset of impacted customers will have notification obligations.

In the coming days, we will provide you with a communications package to support you in engaging with families, teachers and other stakeholders about this incident. The communications package will include tailored outreach emails, talking points, and a robust FAQ so that district and school leadership can confidently discuss this incident with your community.

We understand that you may have additional questions as a result of this update. FAQs are available on PowerSchool Community. Additionally, we will be holding webinars with senior leaders, including our Chief Information Security Officer, to address additional concerns. Please click the link below to register for a webinar that fits your schedule. Note that content for all sessions will be identical, so you need only attend one.

Wednesday, January 8: REGISTER HERE

Thursday, January 9: REGISTER HERE

In the meantime, please reach out to your Customer Success Manager (CSM), Support, or other established PowerSchool contact should you have any questions. We will be sending communications later today to other stakeholders

in your organization who are responsible for other PowerSchool products notifying them of no impact to the other PowerSchool products.

We are addressing the situation in an organized and thorough manner, and we are committed to providing affected customers with the resources and support they may need as we work through this together.

Thank you for your continued support and partnership.

Sincerely,
Hardeep Gulati
Chief Executive Officer

Paul Brook
Chief Customer Officer

cc: **Mishka McCowan**
Chief Information Security Officer