
STAFF LETTER

Subject: PowerSchool Cybersecurity Incident

MPS Staff,

We are writing to inform you of a recent cybersecurity incident involving PowerSchool, a software vendor that provides our Student Information System (SIS). This incident has affected schools and educational institutions globally, underscoring the widespread nature of this event.

On Tuesday, January 7, 2025, PowerSchool informed us of unauthorized access to certain customer data within their system. Importantly, this incident did not involve Mustang Public Schools' servers or internal systems. The breach was specific to PowerSchool's platform, which is used by educational organizations worldwide.

At the time of notification, PowerSchool indicated that their investigation was ongoing and more information would be forthcoming. As a result, we chose to wait until we could verify whether this incident impacted any Mustang-specific data.

During a webinar late last week, PowerSchool confirmed that data from Mustang Public Schools was included in the compromised information. Specifically, the affected data was limited to information stored in PowerSchool's **Teacher Table** and **Student Table**, which include staff demographic information such as address, name, DOB, gender, Local ID, teacher certification number, and MPS email address. Password data is encrypted and not part of this incident, nor are any other systems (enrollment, TalentEd, etc.), according to the webinar.

PowerSchool has further confirmed that while some personally identifiable information (PII), including Social Security numbers (SSNs), was accessed across their customer base, **MPS does not store SSNs in PowerSchool**. However, 14 former employees and one current employee had SSNs stored in the impacted data due to an older archived process. We are in the process of notifying these individuals directly and connecting them with PowerSchool to access resources such as credit monitoring and identity protection services.

We understand the concern and frustration this situation may cause, and we share in that. PowerSchool has provided assurances that the data accessed will not be shared, has been subsequently deleted (with no copy made), and poses no further risk. Additionally, as of 3:00pm today, they have set up a website with information and FAQs: <https://www.powerschool.com/security/sis-incident/>.

Our priority is to keep you informed and support you through this process. As more information becomes available, we will share additional updates. Should you wish to contact PowerSchool directly, the following information is available on their website: 877-873-1550 or Security@PowerSchool.com.

Thank you for your understanding and your continued dedication to the students and families of Mustang Public Schools. While this incident is deeply unfortunate, please know that we are committed to protecting your information and working diligently with PowerSchool to address this matter. We will be in touch as we are provided with additional information.