January 13, 2025

Dear District 200 Families:

This week our school district was informed by PowerSchool of a recent data breach within the PowerSchool Student Information System (PowerSchool SIS). **This breach has had a global impact on its customers, but the company has assured us that District 200 data was not compromised.**

However, we want to share this information, and outline our security procedures and our communication with PowerSchool.

On December 28, 2024, PowerSchool discovered that a threat actor had accessed personnel and student information from customers worldwide using the PowerSchool Student Information System (PowerSchool SIS). The threat actor exploited the user account of a PowerSchool technical support employee, allowing rapid access to millions of records from schools worldwide between December 19 and December 24, 2024.

The privacy and security of personal information are matters of great concern to all of us. We are working with PowerSchool to better understand the scope of the breach and to ensure that appropriate measures are taken to safeguard our data.

Although PowerSchool has assured us that District 200 data was not accessed and the risk of data dissemination or misuse is low, we remain vigilant and are leveraging all available resources to thoroughly assess the situation and strengthen the protection of our systems.

Our school district takes data security very seriously and our Technology Department takes several measures in place to safeguard our systems:

- Two-Factor Authentication: All employee users must verify their identity with a second factor, such as a security key or text message authentication, in addition to their passwords.
- Automated Access Management:  Our PowerSchool system is set up to automatically remove access for employees who leave the district or change positions.
- Best Practices: We follow security best practices, including regular updates, strong password policies and system monitoring to prevent unauthorized access.
- Restricted Remote Access: We have long disabled remote technical support access to mitigate risks from third-party systems, a measure specifically designed to protect against incidents like this.
- Cybersecurity Protection:  We work with a variety of cybersecurity experts at the national and state level to review and enhance our cybersecurity posture.

We appreciate your attention and this opportunity to assure you that our student privacy remains paramount. If you have any questions about this incident or general concerns regarding PowerSchool or student data, please contact our Technology Department  at powerschool@wcusd200.org