Notification of PowerSchool data breach

Dear District 65 families,

On Tuesday, January 7, District 65 was informed by PowerSchool, our Student Information System (SIS), of a recent data breach impacting many of the 18,000 school districts that use PowerSchool nationally. Our staff uses this system daily to access important student demographic and academic information.

I would like to reiterate our district's commitment to maintaining the highest level of privacy and confidentiality regarding student and staff data. We are deeply troubled by this lapse in security and are working closely with PowerSchool as well as other school districts to learn more about what happened.

Over the past two days, our technology team has worked closely with PowerSchool to determine the impact of the breach. While information is still being gathered, we have determined that records of current and former District 65 students were accessed.

What happened?
On December 28, 2024, PowerSchool discovered that a threat actor had accessed personal employee and student information from customers nationwide using the PowerSchool SIS. The threat actor exploited the user account of a PowerSchool technical support employee, allowing access to records from schools nationwide between December 19 and December 24, 2024.

What type of information was accessed at District 65?
Using the instructions provided by PowerSchool, our Technology Department identified the fields accessed at District 65. For all current and former D65 students in PowerSchool, that information includes:

- Student name and District 65 ID number
- Student address
- Student birth date
- Guardian email address
- Transfer dates for the last active school year the student was enrolled
- Student lunch PIN (used only internally)
- Free/reduced lunch status
- Health concerns (examples include allergies; glasses; medical conditions such as asthma, ADHD, epilepsy)

The PowerSchool records accessed for students do **NOT** include grades, GPA, financial information, special education status, schedule information, or Social Security numbers.

What's next?
PowerSchool has informed its customers that they do not anticipate the data being shared or made public, and that they believe it has been deleted without any further replication or dissemination. In addition, PowerSchool has taken the following steps in response to the breach:

- Engaged CrowdStrike, a third-party cybersecurity firm, to investigate the breach. Their final forensic report is expected to be released at the end of next week and will provide a clearer understanding of the incident and its potential impact.
- Implemented additional information security best practices, requiring updated credentials for all employees, and restricting access to their support system tools.

In partnership with the PowerSchool team, District 65 is reviewing our extensive data protection tools and policies to make sure we continue to employ the strongest possible information security protections. While threats of cyberattacks are always a possibility, District 65 employs industry best practices for data storage which includes thorough administrative, physical, and technical safety measures to prevent unauthorized access. We also proactively assess systems for risks and will continue to strengthen systems wherever possible.

District 65 will continue to work with all vendors and partners in taking the necessary precautions to safeguard the personal information entrusted to us by our families. We know that incidents like these are upsetting, and we share your concern. We will continue to share updates as we have them.

If you have any questions, please reach out to me at beardsleys@district65.net.

Sincerely,

Dr. Stacy Beardsley (she/her)
Assistant Superintendent of Performance Management and Accountability

Aviso de violación de datos en PowerSchool

Estimadas familias del Distrito 65,

El martes 7 de enero, el Distrito 65 fue notificado por PowerSchool -nuestro sistema de información estudiantil (SIS)-, de una reciente violación de datos que afectó a muchos de los 18,000 distritos escolares que utilizan PowerSchool a nivel nacional. Nuestro personal utiliza este sistema a diario para tener acceso a información académica y demográfica de los estudiantes que es importante.

Me gustaría reiterar el compromiso de nuestro distrito de mantener el más alto nivel de privacidad y confidencialidad en lo que respecta a los datos de los estudiantes y del personal. Estamos profundamente preocupados por esta falla en la seguridad y estamos Trabajando de cerca con PowerSchool así como con otros distritos escolares para aprender más acerca de lo que sucedió.

Durante los últimos dos días, nuestro equipo de tecnología ha trabajado en estrecha colaboración con PowerSchool para determinar el impacto de la vulneración. Si bien todavía se está recopilando información, hemos determinado que se tuvo acceso a los registros de estudiantes actuales y anteriores del Distrito 65.

¿Qué paso?
El 28 de diciembre del 2024, PowerSchool descubrió que un individuo o grupo dedicados a la piratería informática (hackers) había(n) tenido acceso a información de empleados y estudiantes de sus clientes en todo el país utilizando el 'Sistema de Información Estudiantil' (SIS). El individuo/grupo en cuestión, abusó de la cuenta de usuario de un empleado de soporte técnico de PowerSchool, permitiendo el acceso a registros de escuelas de todo el país entre el 19 y el 24 de diciembre del 2024.

¿Qué tipo de información fue accesada en el Distrito 65?

Utilizando las instrucciones proporcionadas por PowerSchool, nuestro departamento de tecnología identificó los campos a los que se accedió en el Distrito 65. Para todos los estudiantes actuales y anteriores del D65 en PowerSchool, esa información incluye:

- Nombre del estudiante y número de identificación en el Distrito 65
- Domicilio del estudiante
- Fecha de nacimiento del estudiante
- Correo electrónico del tutor
- Fechas de transferencia para el último año escolar activo en el que estuvo inscrito el estudiante
- PIN para almuerzo de estudiantes (utilizado solo internamente)
- Estatus de almuerzo gratuito o a precio reducido
- Preocupaciones de salud (ej: alergias, anteojos, afecciones médicas como asma, TDAH, epilepsia).

Los registros de PowerSchool a los que se tuvo acceso para estudiantes actuales **NO** incluyen calificaciones, GPA, información financiera, estatus de educación especial, información de horarios o números de seguro social.

¿Qué sigue?
PowerSchool ha notificado a sus clientes que no prevén que los datos se compartan o se hagan públicos, y que creen que se han borrado sin que se hayan reproducido ni difundido

más. Además, PowerSchool ha tomado las siguientes medidas en respuesta a su vulneración:

- Se contrató a *CrowdStrike,* una empresa independiente de seguridad cibernética, para que investigara la vulneración. Se espera que su informe forense final sea publicado a finales de la semana próxima y que brinde una comprensión más clara del incidente y de su impacto potencial.
- Implementó mejores prácticas adicionales de seguridad de la información requiriendo credenciales actualizadas para todos los empleados y restringiendo el acceso a sus herramientas del sistema de soporte.

En colaboración con el equipo de PowerSchool, el Distrito 65 está revisando nuestras extensas herramientas y políticas de protección de datos para asegurarnos de que sigamos empleando las protecciones de seguridad de la información más sólidas posibles. Si bien las amenazas de ataques cibernéticos siempre son una posibilidad, el Distrito 65 emplea las mejores prácticas de la industria para el almacenamiento de datos, las cuales incluyen medidas de seguridad administrativas, físicas y técnicas exhaustivas para evitar el acceso no autorizado. También evaluamos de manera proactiva los sistemas en busca de riesgos y continuaremos fortaleciéndolos siempre que sea posible.

El Distrito 65 seguirá trabajando con todos los proveedores y colaboradores para romar las precauciones necesarias para proteger la información personal que nos confían nuestras familias. Sabemos que incidentes como estos son perturbadores y compartimos su preocupación. Seguiremos compartiendo actualizaciones conforme las tengamos.

Si tienen alguna pregunta, por favor, comoníquense conmigo al correo electrónico beardsleys@district65.net.

Atentamente,
Dra. Stacy Beardsley
Subsuperintendente de Administración del desempeño y responsabilidad