Letter received by Orange County Schools from NCDPI (NC Department of Public Instruction)
January 8, 2025

North Carolina Department of
PUBLIC INSTRUCTION

School and District Leaders,

As promised, we wanted to share an update on the PowerSchool cybersecurity incident with you.

On the afternoon of January 7, 2025, PowerSchool notified the North Carolina Department of Public Instruction (NCDPI) and North Carolina public schools about a cybersecurity incident that impacted student and teacher data across their global client base via the PowerSchool Student Information System (SIS). This incident was not isolated to North Carolina.

On December 28, 2024, PowerSchool became aware of a cybersecurity incident that began on December 19, 2024, involving unauthorized access to student and teacher data. The data breach occurred when the credentials of a PowerSchool contract employee were compromised.

PowerSchool and CyberSteward, a professional advisor with deep experience in negotiating with threat actors, have both confirmed that the threat has been contained and the data accessed was destroyed and that no additional copies exist. A full incident report will be provided by CrowdStrike, a third party cybersecurity company working with PowerSchool, after a full analysis.

PowerSchool has indicated that it is not experiencing any operational disruptions and continues to provide services. PowerSchool is working with law enforcement to monitor the dark web for any data exposure.

NCDPI staff has begun conversations with PowerSchool to better understand the impact, if any, on North Carolina students and educators. Our staff is also continuing to analyze the impact on the state.

NCDPI will work alongside PowerSchool, our districts and schools to ensure that all required notifications are conducted. In the coming days, PowerSchool will provide affected customers with a communications package to support them in engaging with families, teachers and other stakeholders about this incident.

North Carolina's public schools do not need to take any technical actions at this time. PowerSchool will continue to provide parent and community communication materials.

It is important to stress that there is nothing that NCDPI or any of our schools could have done to avoid this cybersecurity incident. Neither our schools nor DPI have administrative access to the maintenance tunnel where the breach occurred.

Protecting student and educator data is a top priority, and we are taking this matter very seriously. We will continue to provide support and updates as we learn more.

North Carolina Department of
PUBLIC INSTRUCTION

Stay Connected with North Carolina Public Schools:

Traducción al español de una carta recibida por las Escuelas del Condado de Orange del NCDPI
8 de enero de 2025

Líderes de escuelas y distritos,

Como prometimos, queríamos compartir con ustedes una actualización sobre el incidente de ciberseguridad de PowerSchool.

En la tarde del 7 de enero de 2025, PowerSchool notificó al Departamento de Instrucción Pública de Carolina del Norte (NCDPI) y a las escuelas públicas de Carolina del Norte acerca de un incidente de ciberseguridad que afectó los datos de estudiantes y maestros en toda su base global de clientes a través del Sistema de Información Estudiantil (SIS) de PowerSchool. Este incidente no fue aislado a Carolina del Norte.

El 28 de diciembre de 2024, PowerSchool tuvo conocimiento de un incidente de ciberseguridad que comenzó el 19 de diciembre de 2024 y que implicaba el acceso no autorizado a los datos de estudiantes y profesores. La violación de datos se produjo cuando las credenciales de un empleado contratado por PowerSchool se vieron comprometidas.

Tanto PowerSchool como CyberSteward, un asesor profesional con gran experiencia en la negociación con actores de amenazas, han confirmado que la amenaza ha sido contenida y que los datos a los que se accedió fueron destruidos y que no existen copias adicionales. CrowdStrike, una empresa de ciberseguridad externa que trabaja con PowerSchool, facilitará un informe completo del incidente tras un análisis exhaustivo.

PowerSchool ha indicado que no está experimentando ninguna interrupción operativa y que sigue prestando sus servicios. PowerSchool está trabajando con las fuerzas de seguridad para vigilar la web oscura ("dark web") en busca de cualquier exposición de datos.

El personal del NCDPI ha iniciado conversaciones con PowerSchool para comprender mejor el impacto, si lo hubiera, en los estudiantes y educadores de Carolina del Norte. Nuestro personal también sigue analizando el impacto en el estado.

NCDPI trabajará junto con PowerSchool, nuestros distritos y escuelas para asegurar que todas las notificaciones requeridas se llevan a cabo. En los próximos días, PowerSchool proporcionará a los clientes afectados un paquete de comunicaciones para ayudarles a comunicarse con las familias, los profesores y otras partes interesadas acerca de este incidente.

Las escuelas públicas de Carolina del Norte no necesitan tomar ninguna medida técnica en este momento. PowerSchool seguirá proporcionando materiales de comunicación a los padres y a la comunidad.

Es importante destacar que no hay nada que el NCDPI o cualquiera de nuestras escuelas podría haber hecho para evitar este incidente de seguridad cibernética. Ni nuestras escuelas ni el DPI tienen acceso administrativo al túnel de mantenimiento donde se produjo la brecha.

La protección de los datos de los estudiantes y educadores es una prioridad, y estamos tomando este asunto muy en serio. Seguiremos proporcionando apoyo y actualizaciones a medida que sepamos más.