

**Subject: SOPPA Breach Notice: PowerSchool / Aviso de Violación de Seguridad de SOPPA: PowerSchool**

**Dear Parent(s)/Guardian(s):**

This is a follow up to a communication received on January 10, 2025 and provides additional information on the breach and steps to protect student information. 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. This breach allowed unauthorized access to records between December 19 and December 24, 2024. We regret to inform you that certain data about your child was compromised as part of this national breach.

The following information about your child was accessed:

- 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 internally only)
- Free/reduced lunch status
- Health concerns (e.g., allergies, glasses, medical conditions such as asthma, ADHD, epilepsy)

**Please note:** The accessed records **do not** include grades, GPA, financial information, special education status, schedule information, or Social Security numbers.

The District, in cooperation with PowerSchool, is actively investigating the causes and extent of this breach. PowerSchool has informed us that they do not anticipate the data being shared or made public and believe the information has been deleted without further replication.

The following information and next steps was received directly from PowerSchool on Friday, January 17, 2025:

- **Identity Protection and Credit Monitoring Services:** PowerSchool has engaged Experian, a trusted credit reporting agency, to offer two years of complimentary identity protection services for all students and educators whose information from our PowerSchool SIS was involved. This offer will also include two years of complimentary credit monitoring services for all adult students and educators whose information was involved.
- **Notification to Individuals Involved:** Starting in the next few weeks, in collaboration with Experian, PowerSchool will provide notice to students (or their parents / guardians if the student is under 18) and educators whose information was involved, as well as a phone number to answer any questions you may have about the incident. Enrollment instructions can be found on this website:  
<https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>
- As soon as PowerSchool learned of the incident, they engaged cybersecurity response protocols and mobilized senior leadership and third-party cybersecurity experts to conduct a forensic investigation of the scope of the incident and to monitor for signs of information misuse. PowerSchool is not aware of any identity theft attributable to this incident.

For more information on the PowerSchool data breach, please refer to the communication that was sent to all current District 65 families on January 10, 2025 and visit our district website to learn more about data breaches at: <https://www.district65.net/families/> then click on: Be informed > Student Online Privacy & Safety > Data Breaches. You may also visit <https://www.powerschool.com/security/sis-incident/> for up-to-date information on the cybersecurity incident.

If you have any questions or concerns, please contact:

Dr. Stacy Beardsley

Assistant Superintendent of Performance Management and Accountability

Email: [beardsleys@district65.net](mailto:beardsleys@district65.net)

You may also obtain information from the Federal Trade Commission (FTC) and consumer reporting agencies about fraud alerts and security freezes at:

### **FTC**

[www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes](http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes)

877-FTC-HELP (382-4537)

Federal Trade Commission

600 Pennsylvania Avenue, NW

Washington, DC 20680

### **Equifax**

[www.equifax.com/personal/credit-report-services/](http://www.equifax.com/personal/credit-report-services/)

800-685-1111

Equifax Information Services LLC (fraud alert)

P.O. Box 105069

Atlanta, GA 30348-5069

Equifax Information Services LLC (security freeze)

P.O. Box 105788

Atlanta, GA 30348-5069

### **Experian**

[www.experian.com/help/](http://www.experian.com/help/)

888-EXPERIAN (888-397-3742)

### **Transunion**

<https://www.transunion.com/credit-help>

888-909-8872

Transunion Fraud Victim Assistance (fraud alert)

P.O. Box 2000

Chester, PA 19016

Transunion (security freeze)

P.O. Box 160

Woodlyn, PA 19094

---

**Estimado(s) padre(s)/tutor(es):**

Este es un seguimiento a una comunicación recibida el 10 de enero del 2025 y proporciona información adicional sobre la violación de seguridad y los pasos para proteger la información de los estudiantes. El martes 7 de enero, PowerSchool, nuestro Sistema de Información de Estudiantes (SIS), informó al Distrito 65 sobre una reciente violación de datos que afectó a muchos de los 18,000 distritos escolares que usan PowerSchool a nivel nacional. Esta violación permitió el acceso no autorizado a los registros entre el 19 y el 24 de diciembre de 2024. Lamentamos informarle que ciertos datos sobre su hijo se vieron comprometidos como parte de esta violación de seguridad en todo el país.

Se tuvo acceso a la siguiente información sobre su hijo:

- Nombre del estudiante y número de identificación del Distrito 65
- Dirección del estudiante
- Fecha de nacimiento del estudiante
- Dirección de correo electrónico del tutor
- Fechas de transferencia del último año escolar activo en el que estuvo inscrito el estudiante
- PIN para almuerzo del estudiante (sólo para uso interno)
- Estatus de almuerzo gratuito o reducido
- Problemas de salud (por ejemplo: alergias, anteojos, afecciones médicas como asma, TDAH, epilepsia)

**Por favor, tenga en cuenta:** Los registros a los que se accedió **NO** incluyen calificaciones, GPA, información financiera, estado de educación especial, información de horarios ni números de Seguro Social.

El Distrito, en cooperación con PowerSchool, está investigando activamente las causas y el alcance de esta violación. PowerSchool nos ha informado que no prevén que los datos se compartan ni se hagan públicos y creen que la información se ha eliminado sin más réplicas.

La siguiente información y los pasos a seguir se recibieron directamente de PowerSchool el viernes 17 de enero del 2025:

- **Servicios de protección de identidad y monitoreo de crédito:** PowerSchool ha contratado a Experian, una agencia de informes crediticios de confianza, para ofrecer dos años de servicios de protección de identidad gratuitos para todos los estudiantes y educadores cuya información de nuestro SIS de PowerSchool se vio afectada. Esta oferta también incluirá dos años de servicios de monitoreo crediticio gratuitos para todos los estudiantes y educadores adultos cuya información se vio afectada. Las instrucciones de inscripción se pueden encontrar en este sitio web: <https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/>.
- **Notificación a las personas involucradas:** A partir de las próximas semanas, en colaboración con Experian, PowerSchool enviará un aviso a los estudiantes (o a sus padres o tutores si el estudiante es menor de 18 años) y a los educadores cuya información se vio involucrada, así como un número de teléfono para responder cualquier pregunta que puedan tener sobre el incidente. El aviso incluirá la oferta de servicios de protección de identidad y monitoreo de crédito (según corresponda).
- Tan pronto como PowerSchool se enteró del incidente, puso en marcha protocolos de respuesta de seguridad cibernética y movilizó a la alta dirección y a expertos en seguridad cibernética externos para que llevaran a cabo una investigación forense del alcance del incidente y para controlar si

había indicios de uso indebido de la información. PowerSchool no tiene conocimiento de ningún robo de identidad atribuible a este incidente.

Para obtener más información sobre la violación de datos de PowerSchool, consulte la comunicación que se envió a todas las familias actualmente inscritas en el Distrito 65 el 10 de enero del 2025 y visite el sitio web de nuestro distrito para obtener más información sobre las violaciones de datos en:

<https://www.district65.net/families/> y luego haga clic en las siguientes opciones: Manténgase informado > Privacidad y seguridad en línea de los estudiantes > Violaciones de datos. También puede visitar <https://www.powerschool.com/security/sis-incident/> para obtener información actualizada sobre el incidente de ciberseguridad.

Si tiene alguna pregunta o inquietud, comuníquese con:

Dra. Stacy Beardsley

Subsuperintendente de desempeño administrativo y Contraloría

Email: [beardsleys@district65.net](mailto:beardsleys@district65.net)

También puede obtener información de la Comisión Federal de Comercio (FTC) y de las agencias de informes del consumidor sobre alertas de fraude y congelamientos de seguridad en:

#### **FTC**

[www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes](http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes)

877-FTC-HELP (382-4537)

Comisión Federal de Comercio

600 Pennsylvania Avenue, NW

Washington, DC 20680

#### **Equifax**

[www.equifax.com/personal/credit-report-services/](http://www.equifax.com/personal/credit-report-services/)

800-685-1111

Equifax Information Services LLC (alerta de fraudes)

P.O. Box 105069

Atlanta, GA 30348-5069

Equifax Information Services LLC (congelamiento de seguridad)

P.O. Box 105788

Atlanta, GA 30348-5069

#### **Experian**

[www.experian.com/help/](http://www.experian.com/help/)

888-EXPERIAN (888-397-3742)

#### **Transunion**

<https://www.transunion.com/credit-help>

888-909-8872

Asistencia a víctimas de fraude de Transunion (alerta de fraude)

P.O. Box 2000

Chester, PA 19016

Transunion (congelamiento de seguridad)  
P.O. Box 160  
Woodlyn, PA 19094