Kingsburg Elementary Charter School District

May 14th, 2020

NOTICE OF DATA BREACH

What Happened?	The purpose of this notice is to inform you that our Student Information System had unauthorized access involving your Parent and Student Data. On Tuesday May 12, 2020, the District IT department was notified that several school districts in the surrounding area had recently determined that their SIS (student information system) databases were compromised in November of 2019 through a vulnerability in the Aeries SIS software. Upon receiving this information, our IT department immediately ran security checks, reviewed logs and was able to confirm that Kingsburg Elementary Charter School Districts' Student Information System database was accessed without authorization in November of 2019. Aeries, who licenses our use of the software, notified customers of the following: "In late November 2019, Aeries Software became aware of unauthorized attempts to access data through the Aeries SIS Hosted platform. In response, Aeries immediately began an investigation into whether these attempts had been successful and, if so, how they had been accomplished, what impact, if any, they may have had on data, and what steps they could take to thwart future unauthorized access to data through the Aeries SIS using the same or similar means. At the time, internal investigation did not reveal any compromise of the Aeries SIS or data. Nevertheless, Aeries Software deployed a series of security patches in the December 20, 2019 version of the Aeries SIS which addressed the results of their internal investigation. Then, in late January 2020, Aeries was informed by a locally hosted District that their database may have been previously subject to unauthorized access, they had informed local authorities, and a criminal investigation was underway. Aeries now understands that the investigation by the authorities is ongoing and they are working closely with local law enforcement and federal authorities as well as the original reporting District to determine what transpired, by whom it was perpetrated, and what impact, if any, it may have had on data. In working with the original reporting District and law enforcement officials, in March 2020 Aeries was able to expand their earlier investigation with the new information as to the methods used by the individuals who had accessed data without authorization."

What Information Was Involved?	Student and Parent Internal ID number, First name, Last name, Parent/Guardian name, Residence address, Resident City, Parent/Guardian email address and password.
What We Are Doing.	While there is no evidence to suggest that your data was misused, state law mandates that we notify our families of whose data may have been subject to unauthorized access. (See Cal. Civ. Code § 1798.29; see also Cal. Gov. Code § 6252.) We are instituting a mandatory password reset for all parent and student accounts out of an abundance of caution. Instructions for completing the password reset will be sent to the email address on record for every impacted account. The vulnerability that allowed the data to be exploited was a bug in the Aeries Student Information System software and was patched in December, 2019. We are working with Aeries, and law enforcement where appropriate. Aeries software has indicated the perpetrators have been taken into custody and the unauthorized access has been terminated.
What You Can Do.	We strongly advise all impacted users to follow the instructions being sent out via email to change their Aeries passwords immediately. If you have used your Aeries password for any other online accounts, we strongly advise you to change those passwords as well and avoid using duplicated passwords. There is nothing to suggest that any data was accessed revealing Social Security numbers, credit card numbers, financial account information, or other information directly impacting your credit rating. Nevertheless, If you suspect your personal information has been misused, visit the FTC's site at IdentityTheft.gov to get recovery steps and to file an identity theft complaint. Your complaint will be added to the FTC's Consumer Sentinel Network, where it will be accessible to law enforcers for their investigations.
For More Information.	Call 559-897-2331 or go to https://www.kesd.org/databreach112019

Kingsburg Elementary Charter School District
1310 Stroud Ave
Kingsburg, CA 93631

Kingsburg Elementary Charter School District

14 de mayo, 2020

NOTIFICACIÓN DE FILTRACIÓN DE DATOS

¿Qué pasó?	El propósito de esta noticia es informarle que nuestro Sistema de Información de los Estudiantes tuvo un acceso no autorizado que afecta la información de padres y estudiantes . El martes 12 de mayo, 2020 el IT del Distrito fue notificado que algunos distritos escolares del área habían descubierto que la base de datos de su SIS (Sistema de Información estudiantil) había estado comprometida en noviembre del 2019 a través de una vulnerabilidad en el software SIS de Aeries. Una vez recibida esta información, nuestro departamento de IT inmediatamente hizo algunas pruebas de seguridad y pudo comprobar que el Sistema de Información Estudiantil del Distrito Escolar de Escuelas Primarias de Kingsburg tuvo un acceso no autorizado en noviembre del 2019. Aeries, quien provee el uso del software notificó a sus clientes lo siguiente: “A finales de noviembre del 2019, Aeries Software se dió cuenta de los intentos no autorizados para acceder a la base de datos a través de la plataforma de Aeries SIS. En respuesta, Aeries comenzó una investigación inmediatamente para saber si los intentos se habían llevado a cabo,y si en efecto, como había sucedido y qué impacto, si alguno, había tenido en la información, y que pasos se debÍan seguir para evitar accesos no autorizados en el futuro a través del uso similar a los utilizados por Aeries SIS. Hasta ese momento, la investigación no reveló que la información de Aeries SIS haya estado expuesta. Sin embargo, Aeries Software desplegó una serie de métodos de seguridad en la versión de Aeries SIS del 20 de diciembre del 2019, lo cual resultó en una investigación interna. Más tarde, a finales de enero del 2020, un Distrito local informó a Aeries que su base de datos podría haber tenido un acceso no autorizado previamente, habían informado a las autoridades locales, y había una investigación criminal en marcha. Aeries entiende ahora que la investigación por las autoridades está en proceso y están trabajando de cerca con las autoridades locales y federales así como con el Distrito que reportó el acceso para determinar qué información, quien la perpetró, y qué impacto, si hay alguno, pudo haber tenido en la información. Trabajando con el Distrito que originalmente reportó el acceso y las autoridades, en marzo del 2020 Aeries pudo expandir su investigación previa con más información sobre

	los métodos utilizados por los individuos que habían tenido acceso a la información sin autorización.”
¿Cuál información estuvo involucrada?	Números de ID de los estudiantes y Padres. Nombre, Apellido, Nombre de los Padres/Tutores, Dirección, Ciudad de Residencia, Correo Electrónico y contraseñas de Padres/Tutores.
Que estamos haciendo.	Aún cuando no hay evidencia de que nuestra información esté comprometida, las leyes del estado requiere que notifiquemos a las familias de aquellos a quienes su información haya estado sujeta a un acceso no autorizado (Vea Cal. Civ. Código § 1798.29; también Cal. Gov. Código § 6252.) Estamos requiriendo un cambio mandatorio de contraseñas para todas las cuentas de padres y estudiantes por absoluta precaución. Las instrucciones para cambiar su contraseña le serán enviadas al correo electrónico en nuestros archivos de la cuenta que haya sido expuesta. La vulnerabilidad que permitió que los datos fueran vulnerables fué un error en el software del Sistema de Información Estudiantil de Aeries y fue corregido en diciembre del 2019. Estamos trabajando con Aeries y con las autoridades apropiadamente. Aeries software ha indicado que los delincuentes están bajo custodia y que el acceso no autorizado ha terminado.
Lo que usted puede hacer.	Le recomendamos fuertemente a todos los involucrados que sigan las instrucciones que serán enviadas por correo electrónico para cambiar su contraseña en su cuenta de Aeries inmediatamente. Si usted ha usado la misma contraseña de Aeries para otra cuenta en línea, le aconsejamos que cambie esas contraseñas también y evite usar contraseñas duplicadas. No hay nada que sugiera que la información accedida revelara números de Seguro Social, números de tarjetas de crédito, información de cuentas financieras, u otra información que afecte directamente su crédito. Sin embargo, si sospecha que su información ha sido mal utilizada, visite el FTC’s site en IdentityTheft.gov para obtener los pasos a seguir para llenar una queja de robo de identidad. Su queja sera añadida a la base de datos de Consumer Sentinel de la FTC, donde las autoridades y sus investigadores tendrán acceso a ella.
Para más Información.	Llame al 559-897-2331 o visite https://www.kesd.org/databreach112019

Distrito Escolar de Escuelas Primarias de Kingsburg
1310 Stroud Ave
Kingsburg, CA 93631