

NOTICE OF DATA BREACH

«PG»
«RAD»
«RCY» «ST» «ZC»

Dear Parent of «FN» «LN»

Red Bluff Joint Union High School District (the “District”) is committed to protecting the confidentiality and security of our students’ information and that of their parents. We are writing to address a recent incident that may have involved your data. This notice explains the incident, measures that have been taken, and some steps you can take in response.

What Happened?

The District uses the Aeries Student Information System to provide students and their parents with online access to information regarding school events and schedules. In late November 2019, Aeries learned that an unauthorized individual attempted to exploit a vulnerability in the Aeries software that would allow access to student and parent information. Aeries later determined that the exploit was successful. Upon discovery, Aeries began an investigation and law enforcement launched an investigation to identify the person responsible, who Aeries believes is now in police custody. On May 3rd, 2020, we learned that this individual may have accessed the District’s Aeries System. We then conducted our own investigation, and on May 6th, 2020, determined that the individual did access parent and student data in the District’s Aeries System.

What Information Was Involved?

The information accessible to the perpetrator potentially included parent and/or student name, home address, phone number, email address and hashed password -a form of rendering the actual password indecipherable to third parties – for the Aeries System. The following email accounts associated with your student were affected: «ACCOUNTS»

What You Can Do

Even though we have no evidence that your personal information has been misused, we wanted to let you know this happened and assure you we take it very seriously. Even though the password itself was not accessed, it is possible that an individual with enough time and skill could eventually decipher the password. Therefore, out of an abundance of caution, we recommend you change your password the next time you sign into your account. Additionally, if you use the same password for other online accounts, we recommend changing the password for those accounts as well.

What We Are Doing

We understand the importance of protecting the privacy and security of personal information, and we regret any inconvenience or concern this incident may cause. In order to avoid the possibility of

unauthorized access to the accounts involved, we are recommending all account holders whose accounts were involved to change their passwords. To help prevent something like this from happening again in the future, we installed the software patch that Aeries made available to remedy the vulnerability that allowed the unauthorized individual to potentially access our Aeries system. In addition, we and Aeries are reviewing our existing policies and procedures to mitigate any risk associated with this incident and to better prevent future incidents.

For More Information

We apologize for any inconvenience this may cause you. If you have any questions, please call the district office at 530-529-8704, or email questions@rbhsd.org.

Sincerely,
Todd Brose Superintendent