Da Vinci Schools

201 N. Douglas St., El Segundo, CA 90245 • Phone (310) 725-5800 • www.davincischools.org

NOTICE OF DATA BREACH

MAY 25, 2017

We are writing to inform you of an April 4, 2017 incident in which a limited amount of information about our students stored with one of our data management vendors was very briefly accessed and then deleted by a single individual, who has been referred to by the media as a "white hat" computer security researcher who helps organizations to protect their data.

WHAT HAPPENED?

Wiseburn Unified School District and Da Vinci Schools use a school data platform operated by Schoolzilla PBC Inc. DBA Schoolzilla Inc. ("Schoolzilla") to manage and store information about our students, together with information about their performance on certain exams. In April, we received a Notice of Data Breach from Schoolzilla that described what happened as follows:

"After a recent upgrade to our backup systems, a configuration error exposed Schoolzilla's backup files. A computer security researcher doing targeted vulnerability analysis detected this issue late on April 4, 2017, downloaded those files, and notified us of the problem. As soon as we received the notice on the morning of April 5, 2017, we immediately fixed the error, verified via our log files that nobody other than the one security researcher accessed those exposed files, and ensured that the security researcher who discovered and alerted us to this vulnerability permanently and securely deleted the data."

Schoolzilla informed us that the computer security researcher was not authorized by Schoolzilla to engage in this activity. According to Schoolzilla's CEO, the computer security researcher described "the process by which he stored the data only on his personal hard drive, and then deleted the data and overrode the hard drive using software designed to do that multiple times to ensure the data he possessed for a short time could not be restored. In an affidavit, sworn under penalty of perjury, the researcher affirmed that he has (1) deleted and overwritten the data; (2) not transferred it to, or directly or indirectly shared it with, any other person, source or device; and (3) not used the information for any purpose beyond confirming and demonstrating his access through the discovered vulnerability. He also affirmed in the affidavit that he does not know which school systems' data were included in the download and he has no means to determine that (because all the data has been deleted from his possession and Schoolzilla immediately fixed the vulnerability)." Schoolzilla has informed us that it is unaware of any other unauthorized persons having gained access to Schoolzilla's backup files.

WHAT INFORMATION WAS INVOLVED?

The affected data involved 2015 test scores from the California Assessment of Student Performance and Progress (CAASPP) at Dana Middle School, Burnett Elementary School, and Anza Elementary School and 2015 and 2016 CAASPP test scores from Da Vinci Science and Da Vinci Design. According to Schoolzilla's Notice of Data Breach, "The information involved Schoolzilla's backup files, including school and student data, provided by school district customers, to be managed on our systems. This information includes personally identifiable student information and records…." Our student information stored in Schoolzilla's data platform that was accessed by the unauthorized computer security researcher on April 4, 2017 includes the following: (i) Student name, (ii) Local Student ID Number, (iii) Calif. Longitudinal Pupil Achievement Data System (CALPADS) ID Number, (iv) Grade level, (v) Birthdate, (vi) School

district, (vii) School name, (viii) Gender, (ix) Ethnicity code, (x) Parent education level code, (xi) English learner status abbreviation, (xii) Primary language abbreviation, (xiii) Primary disability abbreviation, and (xiv) Smarter Balanced Assessment Consortium (SBAC) California Assessment of Student Performance and Progress (CAASPP) Exam Scores including overall scores, sub-scores and scaled scores. **We do not store social security numbers, driver's license numbers, California identification card numbers, student or parent emails or passwords, or any credit card or financial information in the Schoolzilla data platform.**

WHAT WE ARE DOING

Schoolzilla's Notice of Data Breach states "As you know, we take security seriously. We have reconfigured our systems to fix the vulnerability, changed passwords, ensured that the downloaded data has been deleted and notified all our customers with personal telephone calls and email correspondence and updates. We are working with third-party security experts to help us augment our existing data security practices, and to look for opportunities to increase our current security defenses. We are also working to run what is known as a 'Red Team Exercise,' a drill where internet and data security experts engage in an all-out attempt to gain access to a system so the vendor can fully test and challenge its cybersecurity defenses to ensure its data is protected."

Although this security incident did not involve our local network, we have run additional diagnostics of our firewall protection system to ensure the safety of our student data. We are continuing to communicate with Schoolzilla to monitor its efforts to protect our student's information stored on the Schoolzilla data platform. Please know that we are determined to remain vigilant with all of our data and with our data management vendors. While this incident is unfortunate, please know that we continue to strive to maintain the integrity and safety of all our data.

WHAT YOU CAN DO

Da Vinci Schools, Wiseburn USD and Schoolzilla are available to speak with you and provide any additional information. Please contact us if you have questions (contact information is below). Please keep in mind that Schoolzilla has assured us that the researcher affirmed and swore under penalty of perjury that he deleted all of the records that he downloaded and does not know which school districts' data he had obtained in his process of confirming the vulnerability.

This incident is an opportunity to remind ourselves about important steps we can take to protect our personal data every day. Consider a family plan for digital privacy and protection and talk to your children about these important issues. As more of our world continues to shift towards digital and cloud-based formats, the importance of cybersecurity becomes even greater. We recognize that any type of security breach may induce anxiety. Accordingly, we will do everything that we can within our control to prevent any future unauthorized access to our student's information.

FOR MORE INFORMATION

We will continue to be in regular contact with Schoolzilla and would be happy to answer any further questions. You may call us at (310) 725-4707. You may email Chris Jones at cjones@davincischools.org or cjones@wiseburn.k12.ca.us, Tom Johnstone at tjohnstone@wiseburn.k12.ca.us , or Matt Wunder at mwunder@davincischools.org. In addition, more information is available on the Schoolzilla blog or by email: security@schoolzilla.com.