Middletown Public Schools

Parent / Guardian of

August 19, 2019

Re: Notification of Vendor Security Incident

Dear Parent(s):

On August 5, 2019, we received a notification of a security incident from Pearson Clinical Assessment ("Pearson"). Pearson is a vendor that many school districts in Connecticut and nationwide use for assessment services. In its notification, Pearson informed us that the security incident affected its AIMSweb 1.0 platform, a tool that the Middletown Board of Education uses to track student reading and math assessments. Pearson also informed us that the incident affected a limited number of our students' "directory information" including names and, in some cases, dates of birth. The incident did not involve any Social Security numbers, credit card data, financial information, grades or other educational or assessment information of any Middletown student.

Beginning immediately after discovery, Pearson launched an incident review by outside cybersecurity experts who determined the nature and extent of any data potentially affected. Pearson informed us that the review has resulted in several additional steps that will further enhance data security going forward. Pearson has received no evidence to indicate that there has been any misuse of your child's information.

As a precaution, Pearson is providing credit-monitoring services to our students at no cost. To sign up for this complimentary service, please follow the instructions below:

- Ensure that you enroll by: January 31, 2020 (Your code will not work after this date)
- If the impacted student is (18+) they will use an adult code, otherwise they will use a minor code
- Visit the Experian IdentityWorks website to enroll and provide your activation code

If you are enrolling for an Adult: https://www.experianidworks.com/credit
Provide your activation code: PF7N9N97G

If you are enrolling for a minor: https://www.experianidworks.com/minorplus
Provide your activation code: 4GCYX5C69

If you are redeeming this for a minor, provide your minor's information when prompted

Following signup, you will be covered for up to 12 months. If you have questions about your new credit-monitoring services please contact Experian's customer care team at 866-883-3309 by January 31, 2020. Be prepared to provide engagement number DB12466 as proof of eligibility for the identity restoration services by Experian.

We take the privacy of student information very seriously and expect our vendors do the same. If you have any questions, please call (860) 638-1429 during the hours of 8:00AM to 4:00PM EST or contact us via email at skottm@mpsct.org.

Sincerely,
Michael Skott
Middletown Board of Education

Information for the Middletown Community
Regarding Pearson Data Security Incident
(Updated August 27, 2019)

As recently reported in national news outlets, Pearson Clinical Assessment, an international company that provides assessment-related products and services to school districts, announced that it suffered a data security incident affecting student information from 13,000 schools and universities. On August 5, 2019, the District received preliminary notification that some, but not all, Middletown students were affected by the Pearson security incident.

The Pearson security incident involved unauthorized access to limited information -- the first and last names and dates of birth -- of certain Middletown students. The incident did not involve access to any of the following information:

Student Social Security numbers (which were not provided to Pearson);
Student grades or other academic information;
Student assessment results;
Student email addresses;
Information related to students' parents or other family members.

Upon learning that Middletown students were affected by the Pearson security incident, the District mobilized technology personnel and resources to implement an incident response plan. The District received a list of affected students from Pearson on August 5, 2019. Upon receipt of this information, the District sent electronic notices to the families of Middletown students who were affected on August 27th. The District is also working with its legal counsel to examine its legal options in light of the security incident and Pearson's response to the same.

The District is providing this set of Frequently Asked Questions ("FAQ") as part of its commitment to keeping parents and the school community informed about the Pearson security incident and its effect on Middletown students. The District will update this set of FAQs as additional information becomes available. District personnel will also continue to directly respond to questions received. Parents and community members with questions may contact Michael Skott skottm@mpsct.org.

FREQUENTLY ASKED QUESTIONS

Which Pearson products and services were the subject of the security incident?

The security incident involved Pearson's AIMSweb platform ("AIMSweb"). AIMSweb is a web-based resource that many school districts, including the Middletown Public Schools, use to monitor students' academic progress in reading and math. The version of the product impacted by the security incident is AIMSweb 1.0. According to Pearson, none of its other products were affected.

How is AIMSweb used in Middletown?

In Middletown, AIMSweb is used for progress monitoring in K-6 grades. The District has utilized AIMSweb as part of its educational program since Fall 2009.

What information is shared with Pearson pursuant to the District's use of AIMSweb?

Pearson has access to the following categories of information regarding students in conjunction with the District's use of AIMSweb: first name, last name, date of birth, student numbers, district name, school name, school year, grade, and teacher name. The District, in accordance with its standard operating principles, disclosed to Pearson the minimum information necessary to operate the software application.

Can you describe the security incident?

The security incident involved unauthorized persons gaining access to certain student information maintained by Pearson in conjunction with its support of the AIMSweb platform. Based on the information received by the District, Pearson became aware of the incident in mid-March 2019. Pearson's investigation determined that the incident occurred in November 2018.

The security incident involved Pearson resources only. None of the District's information technology resources were compromised, or affected in any way, in conjunction with this incident. The security incident affected students in students approximately 13,000 schools and universities across the country.

What student information was affected?

The District has been informed by Pearson that the incident involved unauthorized access to only the first and last names and dates of birth of certain Middletown students. Unlike at many other schools, Middletown student email addresses were not affected, as the District did not provide them to Pearson for this assessment.

The District has been informed that the security incident did not result in unauthorized access to student grades, assessment results or any other academic information. The security incident did not involve access to student's Social Security numbers (Student Social Security numbers are not provided to Pearson). The security incident also did not involve any information related to students' parents or families, as such information is not provided to Pearson.

Can you be sure that student Social Security Numbers were not affected?

Yes. Student Social Security Numbers were never provided to Pearson

What is the scope of the security incident? Was only Middletown affected?

The incident affected more than 13,000 schools and universities across the United States. In Middletown, 7011 students were affected.

How do I know if my child's information has been affected?

Families of Middletown students affected were notified via email on August 27, 2019. The notices were sent with the phrase "AIMSweb Security Incident" in the subject line.

How did the District find out about the security incident?
On August 5, 2019, the District received a preliminary notification that certain Middletown students were affected by the Pearson security incident. On August 5, 2019, the District received an electronic file identifying the affected Middletown students.

What steps has the District taken in response to the incident?

Upon receiving notice that the Pearson security incident affected Middletown students, the District implemented an incident response plan. The Middletown community was alerted through a post to the District web site on August 27, 2019 and families of affected students were notified via email on August 27, 2019.

The District has been in contact with legal counsel as it has implemented the incident response plan and will work with legal counsel to help assess its legal options in light of the security incident and Pearson's response to the same.

What steps has Pearson taken in response to the incident?

The District has been informed that: (a) Pearson has launched an incident review by outside cybersecurity experts who determined the nature and extent of any data potentially affected; (b) Pearson's review has resulted in several additional steps that will further enhance data security going forward; and (c) Pearson has received no evidence to indicate that there has been any misuse of student information. As a precaution, Pearson is providing credit-monitoring services to affected students at no cost through a partnership with Experian.

If my child's information was affected, will I be provided credit monitoring?

Yes. Pearson is providing credit-monitoring services to affected students at no cost for 12 months through a partnership with Experian. This service is being provided out of an abundance of caution, as Pearson has indicted that it has no evidence that the student information was misused or that any financial information or Social Security numbers of any Middletown student was impacted. Instructions on how to register for the free credit monitoring services was emailed to affected families on August 19, 2019.

What rules govern the sharing of student information with Pearson and other vendors?

In 2016, the Connecticut General Assembly enacted a set of student data privacy protections which are considered the most comprehensive in the nation. Any time that the District establishes relationships with outside non-instructional consultants or software / web site operators (collectively, "contractors") which necessitate the sharing of student information, student data, or student-generated content, it must enter into a contract which includes statutorily mandated provisions designed to protect student privacy. For example, contractors must attest that they employ security measures which comply with federal contracting requirements and are consistent with industry standards. Contractors must provide assurances that they are in compliance with federal law regarding the confidentiality of student records, are prohibited from selling and trading student information or using student information for targeted advertising purposes, and must destroy identifiable student information upon request or the expiration of the contract. The law also includes rights of inspection of student data and mandates timely responsive actions in the event of a security incident.

The District has fully complied with the requirements of Connecticut law regarding student data privacy. The District maintains a student data privacy web site with information for parents and community members.

How can I find out which products or companies have access to student information?

The District maintains a list of vendors with whom the District has entered into data sharing agreements on its Student Data Privacy website. The web site includes copies of the student data privacy agreements with approved vendors.

Was the District's network compromised as part of the security incident?

No. No District information technology resources were compromised or affected in any way.

What technical steps does the District take to protect student data privacy?

The District employs multiple layers of protection for the student data it maintains, including the following:

- The placement of Secure Sockets Layer ("SSL") Certificates around access to all student data sites internally hosted;
- Employment of firewalls with malware and antivirus scanning to protect public facing websites and mitigate external threats;
- Use of a segmented network model;
- Encryption of internal authentication transport protocols on user networks;
- Segmentation of guest networks from production / educational networks;
- Encryption of backups;
- Automatic log off / lock users / user desktops;
- Completion of a security audit performed by third party.

As part of its overall network security plan, the District is implementing further security enhancements in conjunction with the upcoming school year.

How can I find out more information about the Pearson security incident?

Please email any additional questions to Michael Skott skottm@mpsct.org.