April 2023

DPO NEWSLETTER

NYSED Date Privacy and Security Updates

Volume 1 Issue 7

Louise DeCandia

Too Much Information

Why does my office share information about what is happening with other States' school districts? Why do so many of us get innumerable notifications every day from federal, State, and private entities telling us about the latest cybersecurity alert? First, we want to be aware of the threat actors threatening our data. Who are they? What is their modus operandi? The more we know, the better prepared we are. Second, there are usually lessons to be learned, especially from other school breaches. Let's take a look at some that have occurred this school year.

Los Angeles started off the school year with a ransomware attack that occurred days before school was scheduled to start in September. School opened on-time making the Superintendent look like an educational superhero. Further, the Superintendent used the national media attention to tell the threat actors that they will not receive a dime. Soon thereafter, 500 gigabytes of data were found on the dark web. The data releases have continued. In February 2,000 student assessment records were posted on the dark web. It appears that the threat actors did not think much of the national attention brought to their ransomware attack. Perhaps, less public negotiations would have been a safer response.

Recently, Denver Public Schools sent notice of an incident that occurred between December 13, 2022, and January 13, 2023. The press has focused on the 58 days it took the school district to notify its staff and students about the breach which included highly sensitive information such as social security numbers, bank account information, student ID's, etc. Many teachers state that they learned about the breach through the news. Although the district insists it complied with the law when making notifications, employees and parents are disappointed in the delayed notification.

Minneapolis Public Schools suffered a ransomware attack in March. The threat actors leaked troves of data going back as far as 1995. The data included grades, budgets, student data, disciplinary records, special education information, student maltreatment, building information and more. Of course, the lesson learned here is that schools should not be holding onto data that it no longer needs to retain.

Three big city American school districts that can provide lessons to all school districts, no the size.

Tanya Davis

I wondered what DPOs should know about Open AI's ChatGPT

So, I asked it. Here is its answer.

As an AI language model, ChatGPT is a tool that can assist educators and students in various ways, such as providing language and research support. However, educational data protection officers should be aware of several key considerations when it comes to using ChatGPT in educational settings:

1. *Data privacy: When using ChatGPT, educators should ensure that any personal or sensitive information is not shared with the model. While ChatGPT does not store data beyond the current conversation, it is still important to protect student privacy and ensure that any data collected is kept secure.*
2. *Bias and fairness: AI language models like ChatGPT are trained on vast amounts of data, and as a result, they may have biases or reinforce stereotypes that exist in the training data. Educators should be aware of this and strive to use ChatGPT in a way that promotes fairness and equality for all students.*
3. *Ethical use: Educational data protection officers should also ensure that ChatGPT is used in an ethical manner that aligns with the school's values and policies. This includes being transparent about its use and limitations and ensuring that its capabilities are not used to harm or discriminate against any students or groups.*

Overall, while ChatGPT can be a valuable tool in educational settings, it is important for educational data protection officers to be aware of its limitations and potential risks, and to do it in a way that prioritizes student privacy and fairness.

Hi again, folks, Tanya here.

The answer reproduced to the left was the second of three that ChatGPT generated at my request. All three were similar, but they did vary in small ways, such as sub-topics and sentence construction. Despite reports of inaccuracy, the information given in response to my query did seem fairly factual when compared with my independent research.

It is important to note that ChatGPT, launched in November 2022, is still in development. Greg Brockman, a cofounder of OpenAI, recently said that launching ChatGPT in its current form was something of a last resort for the company after internal issues with beta testers. Developers have also informed Forbes magazine that the AI costs "millions of dollars a day" to run. So, while ChatGPT may be able to pass the U.S. medical exam, Columbian judges probably shouldn't be using it to write decisions just yet (if ever!).

As with any technology, it is important that students and staff understand ChatGPT's abilities, limitations, and vulnerabilities. ChatGPT can be entertaining (I asked it which was better: peanut butter or jelly, and got fairly entertaining results), but if students are using the platform at all it should only be as a starting point to generate ideas. And no one – students or staff – should be sharing PII with an AI platform. ChatGPT could be excellent fodder for a critical thinking or "check your sources" discussion, but as with any tool, it should be used wisely.