October 2022

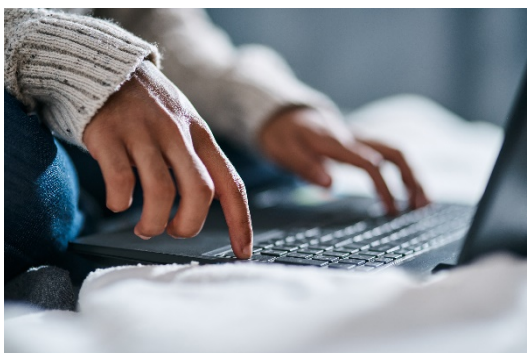
DPO Newsletter

NYSED Data Privacy and Security Updates

Volume 1, Issue 5

Be Aware of the on-line tools your students are using

Are you aware of all the apps your students have uploaded to their school Chromebooks and tablets? Or the apps they are accessing with their school email accounts? If not, it is time to become aware. Some of the newest apps designed to help students manage their class schedules and homework assignments are gathering information about your school's daily schedule and activities directly through students, as well as web scraping a district's website. Using so-called "student ambassadors," these apps collect all types of details about day-to-day activities in schools, such as the school's bell schedule, teacher names, student class schedules (and therefore their location at any point in the day), homework assignments, extracurricular schedules and more. Don't bother to seek an Ed Law 2-d contract with these companies – they are not interested and will tell you they only deal with the students. If your school is not comfortable having all of this information available in a platform that is not under contract with your school, then you may need to intervene.



We advise starting with notifying parents and students about the dangers of using these apps. In addition, check your district's acceptable use policy. Students who sign up for these unauthorized apps might be in violation of your policy (if not, consider updating!). You can also talk to your IT departments about blocking access to certain apps that only allow sign-ups with a student's school email address.

Fall is in the air: October is National Cybersecurity Awareness Month (remember your annual training!)

The leaves are turning color, there is a crispness in the air and the days are getting shorter. Fall is a wonderful season in New York and best of all, October is National Cybersecurity Month! To the DPO, every day is cybersecurity awareness day, but this month brings yet another reason – or excuse – to make your school aware of the importance of good cyber hygiene. Consider circulating an email to all staff informing them that this is National Cybersecurity Month and, in light of recent attacks, such as the attack on the Los Angeles City School District right before the start of the new school year, staff must remain aware and hyper vigilant about your school's cybersecurity. At a minimum, remind staff that they should have strong passwords in place and be aware of phishing attacks. There are numerous National Cybersecurity Awareness Month resources available to help DPOs make the most of this month.
https://www.cisa.gov/cybersecurity-awareness-month
https://www.nist.gov/cybersecurity/cybersecurity-awareness-month

Of course, fall is also the time of year when we train staff on many topics, not the least of which is data privacy and security. As many of you know, I bring up the topic of good data privacy and security training every chance I get. Why? Because studies show that up to 90% of cyber incidents occur due to human error. Indeed, NYSED's 2021 annual report documented that over 50% of the reported data incidents that occurred in schools were due to human error. Recently, we stopped to review the 2022 data incidents filed with my office to date, which have increased dramatically since last year (in part due to the Illuminate Education breach). As of September 15, 2022, 55 data incident reports occurred within the school district (meaning a third-party contractor was not involved). Of those 55, 42 were due to human error. I encourage you to read "Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022." This report seeks to help close the gap on understanding human cybersecurity behavior and offers great (and snarky) insight into the interplay of human behavior and technology.
https://staysafeonline.org/online-safety-privacy-basics/oh-behave/