A Message from our CPO

Happy Summer Everyone!

Although we all know that, even when school is closed, the world of data privacy and security takes no vacations, I hope you all find time to wind-down, relax and enjoy some of the beautiful weather we've been having. In this newsletter, we remind our DPOs that educational agencies must ensure secure return or deletion of data when a third party contract ends. It happens all too often, a breach occurs, a school thinks they are in the clear because their contract ended with that provider years earlier. Then the notice comes in the mail – your school's data has been breached! This can be avoided by having clear contract terms about data retention, destruction and/or return and then following through once a contract term is completed. Relying solely on the third party contractor is a breach waiting to happen. Put your mind at ease and lessen your chances of a breach by ensuring your educational agency's third party contractors are destroying or returning student data in accordance with the terms

Third party contract finished? Make sure the data is destroyed!

As we have learned from recent high profile breaches, third party contractors do not always destroy student data when a contract ends. Education Law § 2-d and Part 121 of the Regulations of the Commissioner of Education require educational agencies that share student data with a third party contractor to ensure that the student data is returned to the educational agency or securely destroyed when there is no further need for the third party contractor to have access to it.

Don't rely on a contract provision that requires the third party contractor to delete student data to meet statutory obligations. The key to success here is being proactive and requiring proof that the third party contractor and any subcontractors securely deleted the data. The easiest way to obtain proof is to require the contractor and any sub-contractors to execute a Certificate of Sanitation, which can be found in NIST SP 800-88.

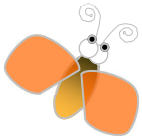
PTAC also provides Best Practices for Data Destruction, which can be found at https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Best%20Practices%20for%20Data%20Destruction%20%282019-3-26%29.pdf

How to change an Educational Agency's Data Protection Officer (DPO)

The privacy office frequently receives questions regarding how to change the registered DPO. Although the answer can be found on our website at: http://www.nysed.gov/data-privacy-security/data-protection-officer-resources, we are including the procedure below:

To register or replace a DPO, the school district, or for charter and 853 schools, the school must send a letter on letterhead to datasupport@nysed.gov. The letter should include the DPO's name, email address and phone number. If the DPO is being replaced, the letter should also include the former DPO's name. This procedure is very similar to the process outlined at: http://www.oms.nysed.gov/sedref/home.html.

If you want to check on DPO registration, visit NYSED Public Reports Portal (https://eservices.nysed.gov/sedreports/list?id=1), the registered DPO list is the fourth item on the reports list.



Get Ready for Next Year Now!

Summer is great… sun, vacation, longer daylight hours, and the opportunity to get your digital resources ready for next year! Restricting student access to downloads and browser extensions is an important step toward protecting their data and your education agency's network.

If an educational agency is not restricting access to downloads and browser extensions, then it is not doing everything possible to protect student data. Additionally, the educational agency runs the risk that an app containing malware may be downloaded by a student who connects to the school network and infects the entire network.

Google Configuration for Schools

The Google Workspace for Education Quickstart IT Setup Guide provides instructions for configuring student accounts. Google Workspace Admin Help also provides guidance such as setting up controls for third-party & internal apps access to Google Workspace data, which can be found at this link: https://support.google.com/a/answer/7281227?hl=en&ref_topic=7558663#zippy=%2Cmanage-access-to-google-services-restricted-or-unrestricted.

Apple Device Configuration

If your educational agency deploys Apple devices, Apple allows user accounts to be restricted so that they cannot download from the App Store, or iTunes Store, autofill web forms, play multiplayer games in Game Center or add extensions to Safari. The Apple Deployment Guide for Education provides a great deal of information and links to help you deploy secure devices that protect student data. The guide is available at this link: https://support.apple.com/guide/deployment-education/welcome/1/web

Microsoft M365 Education Configuration

If your educational agency uses M365 in the cloud, Microsoft has a deployment guide to help make it easier to protect student data. Microsoft walks system administrators through the steps to restrict students from downloading apps and browser extensions and provides additional documentation for administrators who want to learn more. The deployment guide can be found at this link: https://docs.microsoft.com/en-us/microsoft-365/education/deploy/ and the additional documentation can be found at this link: https://docs.microsoft.com/en-us/education/.