NYSED Privacy Office Newsletter

January 2022
Volume 1 Issue 1

Dear DPOs,

Happy New Year! The New Year will see changes in the Office of the Chief Privacy Officer. As you can see from the heading, our office will now be known as the NYSED Privacy Office.

Beginning this month, our office will be sending quarterly newsletters to the Data Protection Officers. This newsletter is our first!

The topic of this month's newsletter is data breaches.

As we start the new year, NYSED's Privacy Office would like to help renew efforts to prevent data breaches by sharing the top 5 most common incidents attributable to human error that are reported to our office, which are:

1. Need to Know
2. Access
3. Use Caution
4. Thoroughly Wipe Old Hardware
5. Pause Before Hitting "Send"

NYSED's Privacy Office wishes all of you a healthy and secure New Year.

Reporting Reminder

The Privacy Office would like to remind you that you are required to report all data incidents to our office. Since 2019, our office has received 239 incident reports from educational agencies and New York State Cyber Command. As a reminder, education agencies are required to report all data incidents affecting student data and/or teacher/principal APPR data suffered by either the educational agency or a third party contractor, to our office within ten days of either the data incident's discovery or receipt of notice of the data incident provided by a third party contractor. Notifying Cyber Command does not relieve you of your obligation to notify our office. Additionally, when student data and/or teacher/principal APPR data has been accessed, disclosed, published or otherwise revealed to any person other than the data subject, school officials with a need to know, or third party contractors in accordance with their specific agreements with the educational agency, Education Law § 2-d requires the adversely affected educational agency to provide notice of the data incident to the affected eligible students, the parents of affected students, and affected teachers and principals.

1. **NEED TO KNOW**

A common error is not employing the principle of least privilege when authorizing access to shared network or cloud drives and folders. Student data and teacher/principal APPR data should only be available to education agency employees with an educational need to know. Additionally, student data should only be available to the subject student and that student's parents, guardians, or persons in parental relation to the student. Take time to check the permissions for shared network and cloud drives and folders to make sure they do not provide access to people who should not receive access.

2. **ACCESS**

Accounts are often misconfigured when created, enabling the account holder to access information the account holder should not be able to access.

3. **USE CAUTION**

Before sending student data home with students, make sure that the information is given to the correct student. In the past 3 years, NYSED's privacy office has received at least 5 incident reports stating that student information was sent home with the wrong student.

4. **THOROUGHLY WIPE OLD HARDWARE**

Before disposing of or selling surplus computers, drives and other equipment, make certain that drive (s) or media containing protected data have been securely wiped in accordance with your Data Privacy and Security Policy. In the past 3 years, NYSED's Privacy Office has received reports from at least 3 educational agencies that sold computer equipment without ensuring that the drive(s) or media that contained protected Student Data and/or Teacher/Principal APPR Data were securely wiped.

5. **PAUSE BEFORE HITTING "SEND"**

Before sending an email that includes student data and/or teacher/principal APPR Data, make certain that the recipients are authorized to receive the data. Unfortunately, this error happens too frequently. Almost half of the incident reports to NYSED's Privacy Office relate to emails that were sent to unintended recipients. This error is easy to make, and procedures should be put in place to mitigate the risk that the error will occur in the future.

These errors *can* happen to you.

In the past 3 years, NYSED's privacy office has received 19 incident reports for inadvertent disclosures due to improper permissions being set for folders and/or drive/server shares. These incidents include:

- A parent who was helping a student with assignments discovered that the student's account had access to other student data stored on the school district's Google drive.
- When Student A's SchoolTool account was created, he was mistakenly connected to a classmate. When the classmate logged into SchoolTool to view his information, he was able to see Student A's.
- The parent of a student attempted to obtain the student's code to use an application. When the parent clicked on the link provided to obtain the code, the parent was able to access the names, student identification numbers, parent names, addresses, and application access codes for the entire class.
- A link to a Google sheet was shared with parents. Unfortunately, the Google sheet was accessible by any person on the Internet with the link.
- G Suite permissions were misconfigured with the permission "share with all" allowing students and staff with no educational need to know to access and view files containing student data.
- While relocating a file containing student data from one shared folder to another, the file's access rules were changed allowing individuals without authorization to view the file.