
In the Matter of
A Privacy Complaint
Filed Against

Review and Determination by
New York State Education Dept.
Chief Privacy Officer

Jericho Union Free School District

On March 12, 2022, a complaint was filed with the New York State Education Department's (NYSED) Chief Privacy Officer by a parent (complainant), whose child attends Jericho Union Free School District (District). Complainant alleges that, in May 2020, students attending the District took photos (screenshot) of a guidance department spreadsheet. Complainant further alleges that these students subsequently disclosed student personally identifiable information (PII), such as whether students attended group counseling and if they are students with a disability, by emailing the screenshot to others. Complainant indicates that they were only provided information about the release of this information by phone calls with the District. Complainant requests a "clear write-up of the situation."

In response to the complaint, on March 18, 2022, NYSED's Chief Privacy Officer requested that the school investigate and issue a written response that summarized its investigation and answered the specific questions or issues listed as (a) through (m) in the letter. The school submitted its response on April 25, 2022.

Applicable Law

The federal Family Educational Rights and Privacy Act (FERPA)[1] protects the privacy of student educational records and places restrictions on the release of students' PII. New York has adopted additional privacy laws and regulations. Education Law § 2-d protects PII from unauthorized disclosure and provides parents with rights regarding their child's PII, especially as pertains to third party contractors.

In accordance with the requirements of Education Law § 2-d, NYSED has adopted a § 2-d Bill of Rights for Data Privacy and Security that authorizes NYSED's Chief Privacy Officer to address complaints about possible breaches and unauthorized disclosure of student PII.

[1] 20 USC § 1232g; 34 CFR Part 99.

District Response

The District states that it did not become aware of the data breach until February 13, 2022. It explains that the breach pertained to an "articulation document" from June 2020 that contained information regarding the incoming high school class of 2024. Every incoming student's information, 286 students in all, was included in this document. It contained PII such as whether a student was a student with a disability, English language learner, 504 status, at risk for SEL, at risk academically, displaced, or qualified for free or reduced price lunch.

The District thereafter discovered that, in June 2020, a guidance counselor inadvertently shared a link to the articulation document with 45 students, mistakenly assuming that the link to the articulation document could not be viewed by anyone other than District staff. The 45 students were subsequently asked via email to "disregard" the message. The District does not indicate whether it checked the security of the link to the articulation document, checked its log files to determine if any of the 45 students accessed the file, or followed up to ensure that the email was securely deleted.

On February 13, 2022, a parent informed the District that "a confidential document on Google sheets had been accessed by students." The parent further indicated that she/he "was in possession of screenshots but did not have access to the confidential document," and "was given the screenshots by his/her [child], whose name was listed on the document."

The District conducted an investigation led by its director of technology. The District states that, "to its knowledge," it determined the student who had originally captured the articulation document in a screenshot; traced all subsequent sharing of the screenshots; and ensured that the screenshots were deleted from students' cameras. The District determined that "each affected family would be contacted by a phone call with a detailed explanation of the data breach[,] including when and how it happened as well as what information was inadvertently shared." The District did not clarify the criteria it used to determine who was an "affected family."

Analysis

Section 121.4 of the regulations of the Commissioner of Education and NYSED's § 2-d Bill of Rights for Data Privacy and Security, allow parents, eligible students, teachers, principals or other staff of an educational agency to file complaints about possible breaches and unauthorized releases of personally identifiable information. Complainant is the parent of a student who attends the District and NYSED's privacy office may therefore address the complaint. Of note, however, no complaint was initially filed with the District. This may be because the District's Parents' Bill of Rights only provides information to parents about filing a complaint

with my office. I remind the District that it is obligated, in accordance with § 121.4 of the regulations of the Commissioner of Education, to establish and communicate to parents, eligible students, teachers, principals and other staff its procedures to file complaints about breaches or unauthorized releases of student data and/or teacher or principal data.

Additionally, the District's investigation was inadequate under the circumstances. When the District learned that a link with student information was inadvertently sent to 45 students in June 2020, it should have, at minimum, determined whether the link was accessible to the 45 students; whether these students opened the link; and whether—and, if so, when and how—these students deleted the email containing the link. Merely requesting that students "disregard" the email was insufficient.

Moreover, the District failed to file a data incident report when this breach first occurred in 2020. Even if the District did not become aware of the breach until February 13, 2022, as it alleges, it was required to report the data breach to my office no later than ten calendar days thereafter (§ 121.10 [d]). No such report appears among the Privacy Office's data incident report filings for 2022. Therefore, the District is required to file a data incident report within five days of this determination.

The District's response further states that "it was decided that the counselors would contact each affected family by phone call with a detailed explanation of the data breach...." After seeking clarification, the District informed my office that the "affected families" encompassed 200 of the 286 students from the class of 2024, each of whom had notations next to their names in the articulation document. Breach notifications must comply with § 121.10 (g) and (h) of the regulations of the Commissioner of Education, which require that:

> (g) notifications ... be clear, concise, use language that is plain and easy to understand, and to the extent available, include: a brief description of the breach of unauthorized release, the dates the incident and the date of the discovery; if known: a description of the types of personally identifiable information affected; an estimate of the number of records affected; a brief description of the educational agency's investigation or plan to investigate; and contact information for representatives who can assist parents or eligible students that have additional questions.
>
> (h) Notification must be directly provided to the affected parent, eligible student, teacher or principal by first class mail to their last known address, by email or by telephone.

The District notified complainant by telephone, as permitted by § 121.10 (h). However, this did not absolve it from the responsibility to convey each category of information required by § 121.10 (g). Relatedly, educational agencies providing notice by telephone must make a representative available to answer additional questions, another requirement contained in §121.10 (g). The District does not dispute that it did not provide additional information in response to Complainant's request thereto.

The instant complaint demonstrates the necessity of the requirements contained in § 121.10 (g). Complainant states that they "do not know how the information was used and who it was sent to in the past two years" and ha[s] no clarity on why this was only discovered now." Complaint states that they would like a clear summary of the situation and steps [the District is] taking to make sure it never happens again."

Therefore, I hereby require the District to provide written notification to complainant addressing all of the requirements listed in §121.10 (g) within 10 calendar days of this determination, which shall be sent to complainant via first class mail.

Determination

The District must review its policies concerning the required actions when an unauthorized disclosure, unauthorized release or breach occurs, in particular the notification requirements in § 121.10. Additionally, the District is required to take the following actions:

1) The District must file a data incident report with my office within five days of this decision. The data incident reporting form is available on NYSED's data privacy and security web page.
2) The District must provide written notification to complainant addressing all of the requirements listed in §121.10 (g). This notification is to be made within 10 calendar days of this determination and sent to complainant via first class mail.
3) No later than May 15, 2022, the District submit evidence to my office that it has come into compliance with § 121.4 of the regulations of the Commissioner of Education by establishing and communicating with parents, eligible students, teachers, principals, and other staff regarding the procedures by which a parent may file complaints about breaches or unauthorized releases of student data and/or teacher or principal data as reflected in the Parent's Bill of Rights.

All responses to this determination are to be sent to privacy@nysed.gov.

April 29, 2022

Louise DeCandia
Chief Privacy Officer
New York State Education Department