

The
University of the
Education



State of New York
Department

In the Matter of
A Privacy Complaint
Filed Against

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

Batavia City School District

In May 2023, a complaint was filed with the New York State Education Department's ("NYSED's") Chief Privacy Officer by a parent ("Complainant"), whose child ("student") attends Batavia City School District ("District"). Complainant states that an employee of the District inappropriately disclosed personally identifiable information ("PII") regarding the student to an emergency contact who was not a legal parent/guardian and was not authorized to receive such PII. Complainant alleges this is a violation of the Family Educational Rights Privacy Act ("FERPA") and Education Law § 2-d.

In response to the complaint, NYSED's Chief Privacy Officer requested that the District investigate and provide a written response, including a summary of its investigation and addressing specific questions and issues. The District submitted its response on June 28, 2023.

Applicable Law

FERPA¹ protects the privacy of student educational records and places restrictions on the release of student PII. New York has adopted additional privacy laws and regulations. Education Law § 2-d, for example,² protects PII from unauthorized disclosure and provides parents with rights regarding their child's PII, especially as it 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 parent complaints about possible breaches and

¹ 20 USC § 1232g; 34 CFR Part 99.

² Education Law § 2-d.

unauthorized disclosure of PII. Section 121.1 (a) of the Regulations of the Commissioner of Education defines a breach as the “unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.” Section 121.1 (t) of the Commissioner’s Regulations defines an unauthorized disclosure or release as “any disclosure or release not permitted by federal or State statute or regulation, any lawful contract or written agreement, or [a disclosure] that does not respond to a lawful order of a court or tribunal or other lawful order.”

District Response

The District indicates that it questioned the employee, who admitted speaking to the emergency contact in response to an incident at school and after being unable to reach the Complainant. The District asserts that no PII was shared with the emergency contact and that there was no violation of either FERPA or Education Law § 2-d.

The District further states that it delivers data privacy training to all employees annually and that, the online privacy training, including information on Education Law § 2-d, was “sent to the [employee] for completion.” The District does not indicate whether the data privacy training was actually completed by the employee but does indicate that the employee was expected to leave the District after June 23, 2023, and therefore no further action was taken.

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. The District did not dispute Complainant’s standing to bring this complaint.

The District does not dispute that one of its employees contacted an emergency contact for the student when they were unable to reach the Complainant. However the District asserts that no PII was shared with the emergency contact during the call.

Determination

Section 121.1 (t) of the Commissioner’s Regulations defines an unauthorized disclosure or release as “any disclosure or release not permitted by federal or State

statute or regulation, any lawful contract or written agreement, or [a disclosure] that does not respond to a lawful order of a court or tribunal or other lawful order.” That section also defines protected student data as “personally identifiable information from the student records of an educational agency.” Additionally, while FERPA authorizes the disclosure of PII to school officials, educational agencies must use reasonable methods to ensure that school officials only obtain access to the education records in which they have a legitimate educational interest [34 CFR § 99.31 (a)].

On the information provided, I cannot determine that the employee inappropriately disclosed PII regarding the student to the emergency contact. Although both parties agree that the call was made, Complainant has not reported details regarding what PII was allegedly shared, and the District employee asserts that they merely “informed the contact that he was calling regarding [the student] and needed [Complainant] to contact [the District].”

I note however, that the District’s responses regarding employee data privacy and awareness training was scant. Section 121.7 of the Commissioner’s regulations require that educational agencies, which includes the District, provide annual data privacy and awareness training. The District is responsible for not only offering data privacy and awareness training annually but for ensuring that all employees with access to PII take the training and understand their obligations under FERPA, Education Law § 2-d and other applicable privacy laws. The District should have clear records regarding when training was offered *and taken* by its employees – no less frequently than on an annual basis. Finally, I remind the District that, beginning this fall my office will be monitoring educational agency compliance with FERPA and Education Law § 2-d³. For some educational agencies this monitoring will include requests for information pertaining to their annual data privacy and awareness training. In light of the foregoing, I strongly encourage the District to review and, if necessary update its policies, procedures and implementation regarding its annual data privacy and security awareness training.

August 16, 2023



Louise DeCandia
Chief Privacy Officer
New York State Education Department

³ See <https://www.nysed.gov/sites/default/files/programs/data-privacy-security/nysed-privacy-office-website-monitoring-memo-7.19.23.pdf>