The University of the State of New York
Education Department

----------x

In the Matter of a Privacy Complaint

Filed Against

Review and Determination of the
Chief Privacy Officer

Highland Falls Central School District
----------x

On April 29, 2025, the New York State Education Department's ("NYSED") Privacy Office received a complaint by a parent ("complainant") whose child (the "student") attends the Highland Falls Central School District (the "district"). Complainant states that a message intended to be sent to her individually via Class Dojo, a communication platform, was distributed to the student's entire class of 127 students. Complainant asserts that this message contained the student's personally identifiable information ("PII"), including student discipline information and information pertaining to the Dignity for All Students Act. Complainant alleges that this violates the Family Educational Rights Privacy Act ("FERPA") and Education Law § 2-d.

In response to the complaint, I requested that the district investigate the allegations, provide a written response summarizing its investigation, and address several specific questions and issues. The district submitted its response on May 22, 2025, and responded to additional questions on May 23, 2025.

District Response

The district admits that it was responsible for the unauthorized disclosure of the student's PII. The district explains that its policy stipulates that applications such as Class Dojo "should be used solely for distributing general, school-wide updates" and the district "prohibits the transmission of [PII] through [such] platforms." Nevertheless, an administrator distributed the student's PII in a message via Class Dojo, due to time constraints, after she was unable to reach a parent or guardian by phone. In response to the incident, the administrator was provided additional training and a formal counseling memorandum to remind the administrator of the district's policy regarding communication with parents.

Applicable Law

FERPA[1] protects the privacy of student educational records, and places restrictions upon educational agencies regarding the release of student personally identifiable information (PII). New York has adopted additional privacy laws and regulations[2] that further protect a student's PII from unauthorized disclosure.

In accordance with the requirements of Education Law § 2-d, NYSED adopted a Bill of Rights for Data Privacy and Security that authorizes NYSED's Chief Privacy Officer to address parent complaints about possible breaches and unauthorized disclosure or release of student PII. The Commissioner's regulations define student data as "personally identifiable information from the student records of an educational agency." Section 121.1 (a) of the Commissioner's regulations 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) further 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."

Analysis

The district does not dispute the facts alleged by complainant and admits that the message was inadvertently transmitted to the entire class of 127 students as outlined above. This release of information violates FERPA and constitutes a breach as defined by section 121.1(a) of the Commissioner's regulations. Therefore, the district was required to report the breach to my office no later than 10 calendar days after it learned of the incident (8 NYCRR 121.10[d]). Since it has not yet done so, the district is hereby directed to file a data incident report within five days of this determination. The form can be found in the "educational agencies" section of NYSED's Data Privacy and Security webpage.

Additionally, I strongly encourage the district to revisit its privacy and security training, which should include examples of ways that individual choices can risk the unwarranted disclosure of student PII. Training on data privacy and security is one of the most important, if not *the* most important tool to protect against breaches and data incidents. Indeed, Education Law § 2-d and section 121.7 of the Commissioner's regulations require annual training on state and federal laws that protect PII. Additionally, I urge the district to make staff and administrators aware of its current written policies regarding communications and the transmission of student PII.

[1] 20 USC § 1232g; 34 CFR Pt. 99

[2] Education Law § 2-d & 8 NYCRR Pt.121

Date: June 23, 2025

_____

Whitney Braunlin, Esq.
Acting Chief Privacy Officer
New York State Education Department
89 Washington Avenue
Albany, NY 12234