# DATA PRIVACY AND SECURITY

# 2018 ANNUAL REPORT

Pursuant to NYS Education Law §2-d, the Chief Privacy Officer is required to issue an annual report on (1) data privacy and security activities and progress, (2) the number and disposition of reported breaches, if any, and (3) a summary of any complaints of possible breaches of student data or teacher or principal annual professional performance review data (PII). This report covers the reporting period of January 1 to December 31, 2018.

## I. Summary of Data Privacy and Security Activities and Progress

In 2018, our office continued the work of implementing Education Law §2-d by continuing the work of drafting implementing regulations with the Data Privacy Advisory Council (DPAC) comprised of representatives of the BOCES, RICS, other stakeholders and parent advocates. DPAC's projects and tasks relate to implementing New York's student data privacy law, Education Law §2-d, and securing the privacy and confidentiality of New York state student data.

To seek stakeholder and public input as the Department developed regulations implementing Education Law §2-d, the Chief Privacy Officer sought public input by holding a series of public forums in fourteen locations throughout the state and also accepted submissions electronically. The forums requested input from stakeholders on (i) student data privacy; and (ii) suggestions for possible additions to the Education Law §2-d bill of rights for data privacy and security.

Pursuant to the requirements of Education Law §2-d, the Department continues to maintain a current inventory of data elements it collects on its website. This inventory lists the following: data element name, the data element description, the purpose for collection, the statutory authority for collection, and the intended uses and disclosure of personally identifiable information.

Education Law 2-d requires the Commissioner of the Education Department to promulgate regulations that establish a standard for data security and privacy policies and practices for

educational agencies. With input from stakeholders and nayional and New York state technical experts, the Department has identified the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) v. 1.1 as the required standard. Created by the United States Department of Commerce with collaboration between industry and government, the NIST CSF consists of standards, guidelines, and practices that will help strengthen the data privacy and security posture of educational agencies. The prioritized, flexible, repeatable, and cost-effective approach of the NIST CSF will assist educational agencies in managing cybersecurity-related risk and establish or improve their data privacy and security programs.

The Department continues to maintain the nysed.gov Data Privacy webpage which serves as a means of communicating updates and providing resources to stakeholders. The website includes an electronic form and easy submission process that parents, educators and administrators may utilize to report alleged breaches or unauthorized releases of protected data.

My office continues to serve as a resource for Department employees and our colleagues in district offices, BOCES and RICS as we promote the implementation of sound information practices for the privacy and security of student data or teacher or principal data, and field multiple inquiries from school district teachers, administrators, parents and advocates on a wide range of data privacy concerns.

## II. Summary of Reported Incidents by Educational Agencies

There was one report submitted in this category by multiple educational agencies reporting that a vendor of a third-party software platform had reported that its platform was accessed by an unknown actor who was able to gain access to one URL without authorization. The educational agencies and third party worked together to correct the exposure.

## III. Summary of Complaints

In 2018, our office received and completed the investigation of seven complaints submitted related to the privacy and/or security of their student's data. One complaint received late 2018 is still open. We worked directly with the school superintendent of each district to ensure the complaints were investigated and that the complainant received a resolution. There were no complaints submitted by principals or teachers. Following is a brief description of complaints submitted:

a. A complaint alleged that an educational agency disclosed personally identifiable information to a vendor for a marketing or commercial purpose contrary to the provisions of Education Law and federal law. The Department determined that the disclosure of personally identifiable information in this case was not a violation of Education Law.

b. A complaint alleged that a student's emergency contact information was mailed by a school district to another family in the district that was not authorized to receive it.
c. A complaint alleged that a school district's transportation office provided personally identifiable information to an ex-spouse, in violation of an order of protection previously provided to the school. The school district investigated and reported that no personally identifiable information was provided. However, the District stated that the situation exposed the need to reconcile the special alert student information in its student management system with its transportation routing system. In the future, the District's transportation department would verify the identity of callers that inquire about PII or sensitive information and check to make sure that there are no restrictions.
d. A complaint alleged that a school district disclosed the names of parents and students, phone numbers and addresses while verifying parent candidate and voter eligibility for an election during a Parent's Association elections. The school investigated and reported that the use of information for purposes of validating parent candidate and voter eligibility was proper.
e. A complaint alleged that a school district posted a classroom picture on its website that included the picture of a student contrary to a parent's stated desire. The District investigated and determined that it had followed its policies and the parent's instructions regarding the use of directory information (which included photographs). However, the District removed the posted photograph when requested.
f. A complaint from a parent queried the identity of the individual who initialed the front page of special education progress reports about a student. The BOCES and school district investigated this complaint and identified the person who initialed the report. To aid future transparency, the agencies involved changed their protocol to require that all staff include their full names on progress reports provided to parents.

## IV. Education and Outreach

With increased outreach from my office, there is a greater awareness amongst educational agencies of the support the Data Privacy and Security office can offer, we have seen an increase in reporting and a greater awareness around data privacy and security best practices with the goal of protecting personally identifiable information and increasing transparency to increase the confidence of parents, students and other stakeholders. We are working to develop teaching tools, educational materials and to make reporting of incidents easy.

Temitope Akinyemi

Chief Privacy Officer