COMMUNITY EDUCATION COUNCIL DISTRICT 15
Office:131 Livingston Street, Room 301, Brooklyn, New York 11201
CEC15@schools.nyc.gov | tel. 718-935-4267 | facebook.com/CECD15 | CECD15.org

Resolution To Support Students with Personal Information Compromised in the June 2023 Data Breach

The Community and Citywide Education Councils (CCECs) are composed of parents who have been elected or appointed to serve as stakeholders of NYC School Community Districts, and specific cohorts of students, representing NYC public school students and their families.

Approved on October 10,2023, the following resolution offers CEC15's position regarding the support of students with personal information compromised in the June 2023 data breach:

WHEREAS, the NYCDOE is mandated by the Family Educational Rights and Privacy Act, the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and the Individuals with Disabilities Act, amongst other legislation, to ensure the security and privacy of student and employee records;

WHEREAS, in 2020, the New York State Department of Education adopted Part 121 of the Regulations of the Commissioner of Education, section 2-d of the Education Law, which outlines numerous requirements that all school districts must implement to strengthen data privacy and security and protect personally identifiable information;

WHEREAS, the NYCDOE is required by New York State law, Part 121, section 2-d, to inform all parties affected by the unauthorized release of personally identifiable information within sixty (60) days of discovery of the respective breach;

WHEREAS, school districts in New York consistently demonstrate difficulty with fulfilling their duties to secure the personal identity information of students and staff as noted in an audit of the Privacy and Security of Student Data carried out by New York State Comptroller Thomas DiNapoli in May 2023;

WHEREAS, a breach of the file transfer system of a NYCDOE contracted vendor, MOVEit, took place beginning Memorial Day weekend, May 27-28;

WHEREAS, the New York City Department of Education ("NYCDOE") announced to members of the media on June 23, 2023 that the personal data/records of 45,000 students and an unspecified number of staff members were compromised;

WHEREAS, over 19,000 documents were accessed without authorization during the MOVEit data breach, including:

A. Full names of students, employees, and contracted related service providers
B. Dates of Birth
C. Social Security Numbers of school staff (approximately 9,700 accessed)
D. Residential Addresses
E. Telephone Numbers
F. Students' Online Student Information System (OSIS) numbers
G. Employee identification numbers
H. Information regarding parents, guardians, siblings, and next of kin
I. Documentation of disability and special education service provision
J. Medicaid reports
K. Documentation of home/heritage language
L. Student evaluations and progress reports;

WHEREAS, the documentation available to hackers during the MOVEit data breach is reported to include documents related to third-party related services received by students with Individual Education Programs (IEPs);

And, WHEREAS, a prior data breach in February 2023 of the Personnel Eligibility Tracking System (PETS) affected approximately 80,000 current or former employees of the NYCDOE's contracted occupational therapists, speech therapists, physical therapists, and other related service providers who are employed by NYCDOE partner agencies;

WHEREAS, the affected current or former employees of the NYCDOE's related service provider partner agencies were not notified of the PETS breach until July 2023, five months after its discovery;

WHEREAS, a prior data breach of Illuminate Education servers took place from December 28, 2021 – January 8, 2022, the personal data of 800,000 current and former students were exposed, across 700 NYCDOE schools;

WHEREAS, all NYCDOE contracted vendors are required by section 2-d of the Education Law of the State of New York to use "encryption technology to protect data while in motion or in its custody from unauthorized disclosure using a technology or

methodology specified by the secretary of the United States Department of Health and Human Services in guidance issued under Section 13402(H)(2) of Public Law 111-5;

WHEREAS, the NYCDOE's contracted vendor, Illuminate Education, admitted that the databases where the students' information was stored were *not* encrypted at the time of the data breach;

WHEREAS, the NYCDOE's contracted vendor, Illuminate Education, informed the NYCDOE of the 800,000-student-record data breach on March 25, 2022, more than sixty days *after* the breach was discovered on January 8, 2022;

WHEREAS, the Illuminate Education data (impacting 800,000 students across 700 NYCDOE schools) is reported by the NYCDOE to include:

A. First and last name
B. Students' Online Student Information System (OSIS) numbers
C. School of Attendance
D. Date of Birth
E. Gender
F. Grade Level
G. Race or Ethnicity
H. Home Language
I. Course information
J. Academic Testing information (some students)
K. English Language Learner status (some students)
L. Documentation of disability and special education service provision
M. Whether or not the student is economically disadvantaged;

WHEREAS, the NYCDOE's response to the Illuminate data breach entailed two parts: First, requiring schools to stop using Illuminate by June 30, 2022. Second, "reviewing security procedures taken by other vendors that provide similar services to DOE schools, families, and students;"

WHEREAS, the NYCDOE's response to the Illuminate Education data breach lacked urgency, as demonstrated by the NYCDOE's direction to schools to stop students from using Illuminate software more than six months after the original data breach, and more than three full months after the NYCDOE was informed that the vendor's servers were not encrypted;

WHEREAS, the NYCDOE's response to both the Illuminate data breach and the PETS data breach did not lead to the enactment of sufficient proactive protections for students' and employees' personal data;

WHEREAS, parents of students affected by the MOVEit data breach were sent notifications on August 7, 2023, 68 days after they learned on May 31 that childrens' personal data was exposed;

WHEREAS, NYCDOE employees and third-party special education service providers affected by the MOVEit data breach were sent notifications on August 15, 2023, 80 days after employees' and contracted professionals' personal data was exposed;

WHEREAS, there is still no Parent Bill of Rights or contractual addendum for MOVEit or the company that owns the program, Progress Software, to attest to the privacy and security protections for student data on the DOE website, as New York State law, Part 121, section 2-d, requires;

WHEREAS, this is also the case for many other companies and organizations that the DOE has provided access to sensitive, personal student information, contrary to the law;

WHEREAS, some of these companies for which the PBORs are missing have been shown to use personal student data for commercial or marketing purposes in violation of New York State law, Part 121, section 2-d; including Naviance, and the College Board, contracted for the administration of the PSAT, AP and SAT exams;

WHEREAS, many of the PBORs that are posted are incomplete and insufficient, in that they do not minimize the data collected, do not specify when the data will be deleted, do not require rigorous encryption; and/or do not clearly prohibit the commercialization of the data, as required by law;

WHEREAS, U.S. Federal Trade Commission data reveals that New Yorkers have reported 22,517 identity fraud cases thus far in the 2023 calendar year, with total losses of $88.6 million to New Yorkers in 2022;

WHEREAS, the NYCDOE has a moral and legal duty to exert its full capacity to ensure the security and privacy of children's and employees' personal information, educational records, human resource data, and all other identifying documents;

WHEREAS, **e**ducational technology / software vendors collect a trove of personal information, including student learning data, emotional status, health, disciplinary and disability information, family economic and racial status, and student assessment data;

WHEREAS, the NYCDOE has failed to ensure that the personal student data that companies and organizations can access is minimized and that the data is deleted when it is no longer needed by companies and organizations, even when this is specified in their contracts and their PBORs, including for students who have long graduated;

WHEREAS, students' personal data and performance assessment data is monetized by some of these companies for a variety of purposes, in violation of New York State law, Part 121, section 2-d;

WHEREAS, these companies did not adhere to New York State law, Part 121, section 2-d in terms of encryption (Illuminate Education), storage (Illuminate Education and MOVEit), and transfer (MOVEit) of children's personal identifying information;

WHEREAS, a recent audit from the State Comptroller found that 80% of cybersecurity incident or breach reports from the NYCDOE lacked enough detail for the Comptroller to say if officials informed students and teachers their data was breached within the legally required 60-day timeline, and in more than half of these breaches, the city failed to make the legal deadline to notify the state of a problem;

WHEREAS, the Special Commissioner of Investigation for NYC Schools has repeatedly recommended improved security and privacy protections by DOE of student data;

WHEREAS, the NYCDOE has announced that it will expand online learning, despite the expanded risks to student data privacy that this involves;

THEREFORE BE IT RESOLVED that the Community Education Council of District 15 urges the NYCDOE to comply with the implementation of information security protocols and technologies that meet/exceed industry standards for data security as specified in New York State law, Part 121, section 2-d;

BE IT ALSO RESOLVED that the Community Education Council of District 15 urges the NYCDOE to fully implement the recommendations of New York State Comptroller Thomas DiNapoli in compliance with the New York State policy, and to ensure the privacy and security of students' and employees' data;

BE IT ALSO RESOLVED that the Community Education Council of District 15 urges the NYCDOE to fully comply with Education Law 2D; and ensure that every company and organization that has access to personal student data has an enforceable contract with a PBOR that is posted on the DOE website; and that this PBOR requires data minimization, high levels of encryption at all times, and a date certain by which the data will be deleted as soon as possible, and at the very least when the student leaves the district or graduates;

BE IT ALSO RESOLVED that Community Education Council of District 15 urges the DOE to require their vendors to delete all personal student data at the end of every school year whenever possible;

BE IT ALSO RESOLVED that Community Education Council of District 15 urges NYCDOE to ensure that every contract and PBOR shall clearly prohibit the use of any such data for sale or for any commercial or marketing purposes;.

BE IT ALSO RESOLVED that NYCDOE shall maintain rigorous oversight, so that all organizations and companies with access to personal data adhere to their contracts and agreements, including requiring regular independent privacy and security audits;

BE IT ALSO RESOLVED that Community Education Council of District 15 urges the NYCDOE to fully comply with all the breach notification provisions in the law, including timely notification of the state and all affected families;

BE IT ALSO RESOLVED that Community Education Council of District 15 urges the NYC Comptroller to act according to his authority to refuse to certify any NYCDOE contract with an organization or company if that contract does not fully comply with New York State law, Part 121, section 2-d, including all the provisions outlined above;

BE IT ALSO RESOLVED that Community Education Council of District 15 urges the NYC Comptroller to audit the NYC DOE agreements with vendors already certified to see that they fully comply with the law, and to see that they are posted on the DOE website;

AND THEREFORE BE IT RESOLVED that the Community Education Council of District 15 urges the NYC Comptroller to propose what changes are needed in law or policy to ensure that personal student data is better secured and protected from breaches or abuse.

This Resolution was approved at a CEC15 Business Meeting held on October 10, 2023 by a vote of members present including: Nancy Randall, Donalda Chumney, Leslie King, Hans Arrieta, Lauren Barkan (IEP), Jonathan Davis, Mamun Rashid (ELL), and Danley Vidal.

Of the 8 members present, 8 voted YES,
4 was absent.