INFORMATION AND DATA PRIVACY, SECURITY, BREACH, AND NOTIFICATION REGULATION

This regulation addresses information and data privacy, security, breach, and notification requirements for student, teacher and principal personally identifiable information (PII) under Education Law §2-d as well as private information under State Technology Law §208.

The District will implement the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection and will adopt technologies, safeguards, and practices which align with it, including assessing the District's current cybersecurity state, its target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

Student and Teacher/Principal "Personally Identifiable Information" under Education Law §2-d

A. Definitions

The following terms shall have the following meanings:

1. Biometric record, as applied to student PII, means one or more measurable biological or behavioral characteristics that can be used for automated recognition of person, which includes fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting.

2. Breach means the unauthorized acquisition, access, use, or disclosure of student PII and/or teacher or principal PII by or to a person not authorized to acquire, access, use, or receive the student and/or teacher or principal PII.

3. Disclose or Disclosure mean to permit access to, or the release, transfer, or other communication of PII by any means, including oral, written, or electronic, whether intended or unintended.

4. Eligible student means a student who is eighteen (18) years or older.

5. Parent means a parent, legal guardian, or person in parental relation to a student.

6. Personally Identifiable Information (PII) as applied to students is information that would allow a reasonable person in the school or its' community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Such data includes, but is not limited to: (1) the student's name; (2) the name of the student's parent or other family members; (3) the address of the student or student's family; (4) a personal identifier, such as the student's social security number, student number, or biometric record; (5) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; or (6) information requested by a person who the District reasonably believes knows the identity of the student to whom the education record relates. PII as applied to teachers and principals means personally identifying information included

in annual professional performance review (APPR) data or any other data that is used as a component of APPR, as defined in Education Law §3012-c, except where required to be disclosed under state law and regulations.

7. Third-Party Contractor means any person or entity, other than an educational agency (i.e., a school, school district, BOCES or State Education Department), that receives student, teacher or principal PII from the District pursuant to a contract or other written agreement for purposes of providing services to the District including, but not limited to, data management or storage services, conducting studies for or on behalf of the District, or audit or evaluation of publicly funded programs. This includes an educational partnership organization that receives student, teacher, and/or principal PII from the District to carry out its responsibilities pursuant to Education Law §211-e (for persistently lowest-achieving schools or schools under registration review) and is not an educational agency. This also includes a not-for-profit corporations or other nonprofit organization, other than an educational agency.

B. Complaints of Breaches or Unauthorized Releases of PII

If a parent, eligible student, teacher, principal, or other District employee believes or has evidence that student, teacher or principal PII has been breached or released without authorization, they must submit this complaint in writing to the District. Complaints should be directed to the Data Protection Officer, but may also be received by any District employee. Any District employee who receives a complaint must immediately notify the Data Protection Officer without unreasonable delay, but no more than forty-eight (48) hours after receipt. This complaint process will be communicated to parents, eligible students, teachers, principals, and other District employees.

The District will promptly acknowledge receipt of complaints, commence an investigation, and take the necessary precautions to protect PII. Following its investigation of the complaint, the District will provide the individual who filed the complaint with its findings within a reasonable period of time, but no more than sixty (60) calendar days from the District's receipt of the complaint. If the District requires additional time, or the response may compromise security or impede a law enforcement investigation, the District will provide the individual who filed the complaint with a written explanation that includes the approximate date when the District will respond to the complaint.

The District will maintain a record of all complaints of breaches or unauthorized releases of student data and their disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1.

C. Notification of Student, Teacher, or Principal PII Breaches

If a third-party contractor has a breach or unauthorized release of PII, it will immediately notify the Data Protection Officer in the most expedient way possible, without unreasonable delay, but no more than forty-eight (48) hours after the breach's discovery. The Data Protection Officer shall in turn notify the State Chief Privacy Officer of the breach or unauthorized release no more than ten (10) calendar days after it received the third-party contractor's notification using a form or

format prescribed by the State Education Department. The Data Protection Officer shall also immediately notify the Superintendent of Schools of the third-party contractor's notification.

The Data Protection Officer will report every discovery or report of a breach or unauthorized release of student, teacher, or principal data to the Chief Privacy Officer without unreasonable delay, but no more than ten (10) calendar days after such discovery.

The District will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than sixty (60) calendar days after the discovery of a breach or unauthorized release by the District or the receipt of a notification of a breach or unauthorized release from a third-party contractor. However, if notification would interfere with an ongoing law enforcement investigation or cause further disclosure of PII by disclosing an unfixed security vulnerability, the District will notify parents, eligible students, teachers, and/or principals within seven (7) calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications 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. Notifications shall be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

1. a brief description of the breach or unauthorized release;
2. the dates of the incident and the date of discovery, if known;
3. a description of the types of PII affected;
4. an estimate of the number of records affected;
5. a brief description of the District's investigation or plan to investigate; and
6. contact information for representatives who can assist parents or eligible students with additional questions.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor will pay for or promptly reimburse the District for the full cost of such notification.

The unauthorized acquisition of student social security numbers, student ID numbers, or biometric records, when in combination with personal information such as names or other identifiers, may also constitute a breach under State Technology Law §208 if the information is not encrypted, and the acquisition compromises the security, confidentiality, or integrity of personal information maintained by the District. In that event, the District will not provide a second notice to the affected individuals; however, it will follow the procedures to notify the required state agencies under State Technology Law §208 as outlined in the following section of this regulation.

<u>"Private Information" under State Technology Law §208</u>

A. Definitions

The following terms shall have the following meanings:

1. Private information means either:

a. personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:
   i. social security number;
   ii. driver's license number or non-driver identification card number;
   iii. account number, credit or debit card number, in combination with any required security code, access code, password or other information which would permit access to an individual's financial account;
   iv. account number or credit or debit card number, if that number could be used to access a person's financial account without other information such as a password or code; or
   v. biometric information (data generated by electronic measurements of a person's physical characteristics, such as fingerprint, voice print, or retina or iris image) used to authenticate or ascertain a person's identity; or

b. a user name or email address, along with a password, or security question and answer, that would permit access to an online account.
   Private information does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;

2. Breach of the security of the system means unauthorized acquisition or acquisition without valid authorization of physical or computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the District. Good faith acquisition of personal information by an officer or employee or agent of the District for the purposes of the District is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

B. Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the District will consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as removal of lost or stolen computer, or other device containing information;
2. indications that the information has been downloaded or copied;
3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; and/or
4. any other factors which the district shall deem appropriate and relevant to such determination.

C. Notification of Breaches to Affected Persons

Once it has been determined that a security breach has occurred, the District will take the following steps:

1. If the breach involved computerized data owned or licensed by the District, the District will notify those New York State residents whose private information was, or is reasonably

believed to have been, accessed or acquired by a person without valid authorization. The notice to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and to restore the integrity of the system. The District will consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures.

2. If the breach involved computer data maintained by the District, the District will notify the owner or licensee of the information of the breach immediately following discovery, if the private information was or is reasonably believed to have been accessed or acquired by a person without valid authorization.

Notifications shall include:

1. district contact information;
2. a description of the categories of information that were or are reasonably believed to have been accessed or acquired without authorization;
3. which specific elements of personal or private information were or are reasonably believed to have been acquired; and
4. the telephone number(s) and website(s) of relevant state and federal agencies that provide information on security breach response and identity theft protection and prevention.

Notifications shall be directly provided to the affected individuals by either:

1. written notice;
2. electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form and the District keeps a log of each such electronic notification; or
3. telephone notification, provided that the District keeps a log of each such telephone notification.

However, if the District can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; (b) the number of persons to be notified exceeds 500,000; or (c) the District does not have sufficient contact information, substitute notice may be provided. Substitute notice shall consist of all of the following:

1. email notice when the District has such address for the affected individual;
2. conspicuous posting on the District's website; and
3. notification to major media.

In accordance with the law, the District will not notify individuals if the breach was inadvertently made by individuals authorized to access the information and the District reasonably determines the breach will not result in misuse of the information or financial or emotional harm to the affected persons. The District will document its determination in writing and maintain it for at least five years, and will send it to the State Attorney General within ten (10) days of making the determination.

If the District has already notified affected persons under any other federal or state laws or regulations regarding data breaches, including the federal Health Insurance Portability and Accountability Act, the federal Health Information Technology for Economic and Clinical Health

(HI TECH) Act, or New York State Education Law §2-d, it will not provide a second notice to the affected individuals; however, it will follow the applicable procedures to notify any required state and/or other agencies.

D. Notification to State Agencies and Other Entities

Once notice has been made to affected New York State residents, the District shall notify the State Attorney General, the State Department of State, and the State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

If more than 5,000 New York State residents are to be notified at one time, the District will also notify consumer reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

If the District is required to notify the U.S. Secretary of Health and Human Services of a breach of unsecured protected health information under the federal Health Insurance Portability and Accountability Act (HIPAA) or the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, it will also notify the State Attorney General within five (5) business days of notifying the Secretary.

Adoption date: May 8, 2007
Revised: March 20, 2019
Revised: