VALLEY STREAM UNION FREE SCHOOL DISTRICT TWENTY-FOUR

INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION REGULATION

Policy 6168-R

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.

I. Student, Teacher and Principal Personally Identifiable Information under Education Law § 2-d

A. Definitions

This policy hereby incorporate by reference the definitions contained in Education Law § 2-d and/or its implementing regulations in Part 121 of the Regulations of the Commissioner of Education. The following terms, as used in this policy, will mean:

"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.

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

"*Contract or other written agreement*" means a binding agreement between the District and a third-party, including, but not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

"*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.

"Personally Identifiable Information" as applied to students means personally identifiable information as defined in section 99.3 of Title 34 of the Code of 3 Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 USC § 1232g, which includes the following information for District students:

1. the student's name;
2. the name of the student's parent(s) 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;

6. other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or
7. information requested by a person who the District reasonably believes knows the identity of the student to whom the education record relates.

Additionally, the State Chief Privacy Officer (CPO) has determined that student and parent phone numbers are considered PII.

"*Personally Identifiable Information*" as applied to teacher and/or principals, means results of Annual Professional Performance Reviews (APPR) that identify the individual teachers and/or principals, which are confidential under Education Law §§ 3012-c and 3012-d, except where required to be disclosed under state law and regulations.

"*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 and/or principal PII from the educational agency pursuant to a contract or other written agreement for purposes of providing services to the educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This includes an educational partnership organization that receives student, teacher and/or principal PII from a school 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 includes a not-for-profit corporation or other nonprofit organization, other than an educational agency.

B. Complaints of Breaches or Unauthorized Releases of PII

If a parent/guardian or eligible student wishes to claim student PII has been breached (disclosed, accessed, used or released) without authorization, they must submit this complaint in writing to the district. Complaints may be received by the Data Protection Officer (DPO), but may also be received by any district employee, who must immediately notify the DPO. This complaint process will be communicated to parents and eligible students. All employees are required to report breaches of student, teacher, or principal PII that they are aware of to the DPO.

The District will acknowledge receipt of complaints promptly, 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 a complaint with its findings within a reasonable period of time, no more than 60 calendar days from the receipt of the complaint.

If the District requires additional time, or if the response may compromise security or impede a law enforcement investigation, the District will provide the individual who filed a complaint with a written explanation that includes the approximate date when the District anticipates it 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 and Retention and Disposition Schedule LGS-1.

After going through the District's complaint procedure, parents and eligible students may also submit complaints to the State Education Department's Chief Privacy Officer at privacy@nysed.gov.

C. Notification of Student and Teacher/Principal PII Breaches

If a third-party contractor has a breach or unauthorized release of PII, it will promptly notify the DPO in the most expedient way possible, without unreasonable delay, but no more than seven (7) calendar days after the breach's discovery.

The Superintendent of Schools and/or the DPO will then notify the State Chief Privacy Officer of the breach or unauthorized release no more than ten (10) calendar days after it receives the third-party contractor's notification using a form or format prescribed by the State Education Department.

The DPO 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 may make such report in any manner authorized by law including electronically.

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 or third-party contractor notification.

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

- a brief description of the breach or unauthorized release,
- the dates of the incident and the date of discovery, if known;

- a description of the types of PII affected;
- an estimate of the number of records affected;
- a brief description of the District's investigation or plan to investigate; and
- contact information for representatives who can assist parents or eligible students with additional questions.

Notification 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.

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 is not required to notify affected people twice, but must follow the procedures to notify state agencies under State Technology Law § 208 as outlined in section II of this regulation.

II. "Private Information" under State Technology Law § 208

A. Definitions

"*Private Information*," as defined in State Technology Law § 208, means either:

1. 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 combination of 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 used to authenticate or ascertain a person's identity; or

2. a username 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 publicly available information that is lawfully made available to the general public from federal, state, or local government records.

"*Breach of the security of the system*" means unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the District. Good faith acquisition of personal information by an 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 a 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. Procedures and Methods for Notification of Breaches

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 disclosure 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, and may consult with the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC), 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 will 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, the dates of the incident and the date of discovery, if known;
2. a description of the types of PII affected;
3. an estimate of the number of records affected;
4. a brief description of the District's investigation or plan to investigate;
5. contact information for representatives who can assist parents or eligible students, teachers or principals that have additional questions; and
6. the telephone number and website of relevant state and federal agencies that provide information on security breach response and identity theft protection and prevention.

This notice will 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 that the district keeps a log of each such electronic notification. In no case, however, will the District require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.
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; or (b) that the number of persons to be notified exceeds 500,000; or (c) that the District does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. e-mail 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.

Notification may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. In such an event, the notification will be made after the law enforcement agency determines that such notification no longer compromises the investigation.

However, the District is not required to 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. If the breach affected over 500 residents of New York, the District shall provide the written determination to the State Attorney General within ten 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 is not required to notify them again. Notification to state and other agencies is still required.

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.

Cross Ref.: 6168 Information and Data Privacy, Security, Breach and Notification
Adoption date: April 28, 2026
Classification:
Revised Dates: