VALLEY STREAM UNION FREE SCHOOL DISTRICT TWENTY-FOUR

INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION

Policy 6168

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework (Version 1.1) (NSIT CSF) for data security and protection.

The Data Protection Officer (DPO) is responsible for ensuring the District's systems follow NIST CSF and adopt technologies, safeguards and practices which align with it. This will include an assessment of the District's current cybersecurity state, their target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board will designate a DPO who will be responsible for the implementation and oversight of this policy and any related procedures including, but not limited to, those required by Education Law § 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the District. The appointment will be made at the annual organizational meeting.

The Board of Education directs the Superintendent of Schools or their designee, in accordance with appropriate business and technology personnel, and the DPO (where applicable) to establish regulations which address:

- the protections of personally identifiable information (PII) of students, teachers, and principals under Education Law § 2-d and Part 121 of the Commissioner of Education Regulations;
- the protections of private information under State Technology Law § 208 and the New York SHIELD Act; and
- procedures to notify parents affected by breaches or unauthorized access of protected information.

I. Student and Teacher/Principal Personally Identifiable Information

A. General Provisions

PII as applied to student data is as defined in the Family Educational Rights and Privacy Act (FERPA), which includes certain types of information that could identify a student, and is listed in the accompanying regulation 6168-R. PII as applied to teacher and principal data, means results of Annual Professional Performance Reviews (APPR) that identify the individual teachers and principals, which are confidential under Education Law §§ 3012-c and 3012-d, except where required to be disclosed under state law and regulations.

The Data Protection Officer (DPO) and/or their designee will see that every use and disclosure of PII by the District benefits students and the District by considering, among other criteria, whether the use and/or disclosure will improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations. However, PII will not be included in public reports or other documents.

The District will protect the confidentiality of student, teacher, and principal PII while stored or transferred using industry standard safeguards and best practices, such as multi-factor authentication (MFA), encryption, firewalls, and passwords. The District will monitor its data systems, develop incident response plans, limit access to PII to District employees and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed.

Under no circumstances will the District sell PII. It will not disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by any other party for any marketing or commercial purposes, or permit another party to do so. Further, the District will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law or in the case of enrollment data, the District will not report the following student data to the State Education Department:

1. juvenile delinquency records;
2. criminal records;
3. medical and health records; and
4. student biometric information.

The District has created and adopted a Parent's Bill of Rights for Data Privacy and Security (see Exhibit 6168-E). It is published in the Parent Handbook, on the District's website at https://valleystreamschooldistrict24.org/parent-resources\ and can be requested from the District Clerk.

Nothing in Education Law Section 2-d or this policy should be construed as limiting the administrative use of student, teacher, and/or principal PII by a person acting exclusively in the person's capacity as an employee of the District.

B. Third-party Contractors

The District will ensure that contracts with third-party contractors or separate data sharing and confidentiality agreements require the confidentiality of shared student, teacher, and/or principal PII be maintained in accordance with federal and state law and the District's data security and privacy policy.

If a third-party contractor has a breach or unauthorized release of PII, it will promptly notify the District in the most expedient way possible without unreasonable delay but no more than seven (7) calendar days after the breach's discovery. The District will report the breach to the New York State Department of Education's Chief Privacy Officer within ten (10) days of notification of the breach.

The District will ensure that the contract or written agreement with any third-party contractor includes the third-party contractor's data security and privacy plan. This plan must include a signed copy of the Parent's Bill of Rights and must be accepted by the District.

C. Training

The District will provide annual training on data privacy and security awareness to all employees who have access to student, teacher and/or principal PII.

D. Reporting

Any breach of the District's information storage or computerized data which compromises the security, confidentiality, or integrity of student, teacher, and/or principal PII maintained by the District will be promptly reported to the DPO, the Superintendent, and the Board of Education.

E. Notifications

The District values the protection or private information of individuals in accordance with applicable law and regulations. Further, the District is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy.

The DPO will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the State's Chief Privacy Officer (CPO) 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 of 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.

The Superintendent in consultation with the DPO, will establish procedures to provide notification of a breach or unauthorized release of student, teacher and/or principal PII. The Superintendent and DPO will establish and communicate to parents, eligible students, and District staff a process for filing complaints about breaches or unauthorized releases of student, teacher, and/or principal PII.

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

"Private Information" is defined in State Technology Law § 208, and includes certain types of information, outlined in the accompanying regulation, which would put an individual at risk for identity theft or permit access to private accounts. "Private information" does not include publicly

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

Any breach of the District's information, storage, or computerized data which compromises the security, confidentiality, or integrity of private information maintained by the District must be promptly reported to the Superintendent and the Board of Education.

The Board directs the Superintendent of Schools or their designee, in accordance with appropriate business and technology personnel, and the DPO (where applicable) to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breached of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

III. Employee "Personal Identifying Information" under Labor Law § 203-d

Pursuant to Labor Law § 203-d, the District will not communicate employee personal identifying information (PII) to the general public. This includes:

1. social security number;
2. home address or telephone number;
3. personal email;
4. internet identification name or password;
5. parents' surname prior to marriage; and
6. drivers license number.

In addition, the District will protect employees' social security numbers in that such numbers will not be:

1. publicly posted or displayed;
2. visibly printed on any ID badge, card, or timecard;
3. placed in files with unrestricted access; or
4. used for occupational licensing purposes.

Employees with access to such information will be notified of these prohibitions and their obligations.

Cross-ref: 5130 Access to Student Records
5131 Code of Conduct
5550 Student Privacy under the PPRA

6165 Computer Resources and Data Management
6166 Computer, Network and Internet Acceptable Use
6167 Internet Safety

6168-R Information and Data Privacy, Security, Breach, and Notification Regulation

Ref: State Technology Law §§ 55201-208
Labor Law § 203-d
Educ. Law § 2-d
NYCRR Part 121

Adoption date:

Revised: April 28, 2026