

**SUBJECT: POLICY ON DATA SECURITY AND PRIVACY**

The Board of Education is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the District and when disclosing or releasing Personally Identifiable Information (“PII”) to others. The Board adopts this policy to implement the requirements of Education Law § 2-d and its implementing regulations.

**Parent and Student Rights Under State and Federal Law**

This Policy shall include all protections given to parents/persons in parental relationship and students pursuant all State and federal laws that protect student data, including but not limited to Board policies implementing the Family Educational Rights in Privacy Act and the Americans with Disabilities Act.

**Parents Bill of Rights**

The Superintendent, or designee, shall publish a Parents Bill of Rights in an appropriate location on the District’s website which shall inform parents:

- (1) A student’s personally identifiable information cannot be sold or released for any commercial purposes;
- (2) Parents have the right to inspect and review the complete contents of their child’s education record, and the process for requesting such review;
- (3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;
- (4) A complete list of all student data elements collected by New York State is available for public review on the State’s website, including link to that information, or by writing to the address and individual designated by the State including the contact information; and
- (5) Parents have the right to have complaints about possible breaches of student data addressed, and the process for making such complaints. Complaints should be directed to the Data Protection Officer, with contact information.

**Use and Disclosure of Personally Identifiable Data**

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, the District will take steps to minimize its collection, processing, and transmission of PII. Every use and disclosure of personally identifiable information by the educational agency shall benefit students and the educational agency (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and

effective school operations). No personally identifiable information may be included in public reports or other documents, unless otherwise authorized by law.

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

### **Chief Privacy Officer**

The District will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law § 2-d, its implementing regulations, and this policy.

### **Data Protection Officer**

The Board of Education shall designate a Data Protection Officer who shall be responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law § 2-d and its implementing regulations. The Data Protection Officer will also serve as the main point of contact for data privacy and security for the District.

The Superintendent shall ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities.

### **District Data Privacy and Security Standards**

The District will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) ("Framework") as the standard for its data privacy and security program.

### **Third-Party Contractors**

Any and all contracts between the District and third-party contractors, under which a contractor will receive student data or teacher or principal data, shall include provisions requiring that the contractor maintain the confidentiality of shared student data or teacher or principal data in accordance with law, regulation, and District policy.

In addition, the District will ensure that the contract or written agreement includes a signed copy of the Parents Bill of Rights and the contractor's data privacy and security plan, in compliance with Part 121 of the Commissioner's regulations and that has been accepted by the District.

The District will publish on its website a supplement to the Bill of Rights for any contract or other written agreement it has entered with a third-party contractor that will receive PII from the District. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

Agreements subject to this policy include any agreement created in electronic form and signed with an electronic or digital signature or a click wrap agreement that is 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.

## **Reporting a Breach or Unauthorized Release**

The Superintendent or designee will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the District to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

## **Annual Data Privacy and Security Training**

The Superintendent or designee shall ensure that annual data privacy and security awareness training is provided the District's officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. This training may be delivered using online training tools. Additionally, this training may be included as part of the training that the District already offers to its workforce.

## **Notification of Policy**

This policy will be published on the District's website and a copy shall be given to all officers and staff.

Education Law § 2-d  
8 NYCRR Part 121

Adoption Date