8635 INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION

This Policy addresses the District's responsibility to adopt appropriate administrative, technical, and physical safeguards and controls to protect and maintain the confidentiality, integrity, and availability of its data, data systems, and information technology resources.

This Policy applies to the District's employees, independent contractors, interns, volunteers, and third-party contractors who receive or have access to the District's data and/or data systems ("users").

District and building administrators are responsible for the compliance of their programs and offices with this policy, related policies, and their applicable standards, guidelines, and procedures. Instances of non-compliance will be addressed on a case-by-case basis. All cases will be documented, and program offices will be directed to adopt corrective practices, as applicable.

This Policy encompasses all systems, automated and manual, including systems managed or hosted by third-parties on behalf of the District. It also addresses all information, regardless of the form or format, which is created or used in support of the District's activities.

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 (NIST CSF) for its Data Privacy and Security Program. Either the *Superintendent or Data Privacy Officer* will be 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 establish a Data Governance Team and will designate a Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations to develop and maintain a comprehensive Data Privacy and Security Program. The Data Protection Officer will serve as the point of contact for the Data Privacy and Security Program.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, and the Data Protection Officer (where applicable) to establish regulations which address:

- the collection, retention, dissemination, and protection of "personally identifiable information" and sensitive and confidential information of student and teachers/principal under Education Law §2-d and Part 121 of the Commissioner of Education;
- the protections of "private information" under State Technology Law §208 and the NY SHIELD Act;
- the adherence of its third-party contractors with federal, state, and District requirements in its agreements;
- training users to share a measure of responsibility for protecting the District's data and data systems; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.

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

A. General Provisions

Laws including the Family Educational Rights and Privacy Act (FERPA), Education Law §2-d, and other state or federal laws establish baseline parameters for what is permissible when sharing student PII.

PII as applied to student data is as defined in Family Educational Rights and Privacy Act (Policy 5500), which includes certain types of information that could identify a student, and is listed in the accompanying regulation 8635-R. PII as applied to teacher and principal data, means results of Annual Professional Performance Reviews 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 will see that every use and disclosure of personally identifiable information (PII) by the District benefits students and the District (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations). The Data Privacy Officer and the Data Governance Team will, together with program offices, determine whether a proposed use of PII is not included in public reports or other documents, or otherwise publicly disclosed.

The District will protect the confidentiality of student and teacher/principal PII while stored or transferred using industry standard safeguards and best practices, such as 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.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student

records, as well as permitted disclosures without consent, which are addressed in policy and regulation 5500, Student Records.

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 purpose, 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:
- juvenile delinquency records;
- criminal records;
- medical and health records; and
- student biometric information.

The District has created and adopted a Parent's Bill of Rights for Data Privacy and Security (see Exhibit 8635-E). It has been published on the District's website at http://www.ryeneck.k12.ny.us/ and can be requested from the District Clerk.

B. Third-party Contractors

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

Each third-party contractor that will receive student data or teacher or principal data must:

- adopt technologies, safeguards, and practices that align with the NIST CSF;
- comply with the District's data security and privacy policy and applicable laws impacting the District;
- limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
- not use the PII for any purpose not explicitly authorized in its contract;
- not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older): except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or unless required by statute or court order and the third-party contractor provides notice of disclosure to the District, unless expressly prohibited.
- maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;
- use encryption to protect PII in its custody; and
- not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for marketing or commercial purpose, or permit another party to do so. Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the District.

If the 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 calendar days after the breach's discovery.

C. Third-Party Contractors' Data Security and Privacy Plan

The District will ensure that contracts with all third-party contractors include the third- party contractor's data security and privacy plan. No PII will be shared with the third- party contractors if they do not submit a data security and privacy plan. This plan must be accepted by the district.

At a minimum, each plan will:

- outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with this policy;
- specify the safeguards and practices it has in place to protect PII;
- demonstrate that it complies with the requirements of Section 121.3(c) of this Part;
- specify how those who have access to student and/or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

- specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
- specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
- describe if, how and when data will be returned to the District, transitioned to a successor contractor, at the District's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

D. Training

All users of the District's data, data systems, and data assets must complete annual training on data privacy and security awareness provided by the District.

E. Requests for Personally Identifiable Information

The identity of all individuals requesting PII, even where they claim to be a parent, guardian, eligible student, or data subject must be authenticated in accordance with the District's and SED's procedures.

F. Reporting

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

For purposes of this policy, a breach means the unauthorized acquisition, access, use, or disclosure of student PII and/or teacher or principal PII or any SED sensitive or confidential data or a dta system that stores that data, by or to a person not authorized to acquire, access, use, or receive the data.

G. Incident Responses and Notifications

The District will respond to data privacy and security critical incidents in accordance with this policy.

The Data Privacy Officer 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 without unreasonable delay, but no more than 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 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 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 Data Protection Officer, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and District staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

The Data Privacy Officer must annually report to the Board of Education on data privacy and security activities and progress, the number and disposition of reported breaches, if any, and a summary of any complaints submitted pursuant to Education Law 2-d.

H. Compliance with the District's Acceptable Use Policy For Technology and the Internet

Users must comply with the District's Acceptable Use Policy when using District resources. Access privileges will be granted in accordance with the user's job responsibilities. Access privileges will be limited to the extent necessary to accomplish assigned tasks in accordance with the District's mission and business functions. Access privileges will be discontinued for those who are no longer with the District.

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 information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

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, in accordance with appropriate business and technology personnel, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breaches 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" to the general public. This includes:

- social security number;
- home address or telephone number;
- personal email address;
- Internet identification name or password;
- parent's surname prior to marriage; and
- drivers' license number.

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

- publicly posted or displayed;
- visibly printed on any ID badge, card or time card;
- placed in files with unrestricted access; or
- used for occupational licensing purposes.

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

This policy will be published on the District's website and notice of its existence will be provided to all employees and users.

Cross-ref:

1120, District Records

4526, Internet Safety Policy

5500, Student Records

8630, Computer Resources and Data Management

Ref:

State Technology Law §§201-208

Labor Law §203-d

Education Law §2-d

8 NYCRR Part 121

Adoption date: June 17, 2020

Rye Neck Union Free School District