INFORMATION AND DATA PRIVACY, SECURITY, BREACH, AND NOTIFICATION

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 hereby adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The Superintendent and the Data Protection Officer are responsible for ensuring the District's systems follow NIST CSF and adopting technologies, safeguards, and practices which align with it. This includes 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 Data Protection Officer to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations, and to serve as the point of contact for data security and privacy for the District.

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

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

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

A. General Provisions

Personally identifiable information (PII), as applied to student data, is as defined in the Family Educational Rights and Privacy Act (FERPA) and its implementing regulations, and includes certain information that would allow a person to identify a student. PII, as applied to teacher and principal data, includes 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.

The Data Protection Officer will see that every use and disclosure of 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). PII shall 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 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. The District will also comply with all federal and state laws and regulations regarding confidentiality of and access to student records, as well as permitted disclosures without consent.

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:

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 8635-E). It has been published on the district's website at https://www.yonkerspublicschools.org/Page/1676 and can be requested from the District's Office of Communication.

B. Third-Party Contractors

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

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

1. adopt technologies, safeguards and practices that align with the NIST CSF;
2. comply with the District's data security and privacy policy and applicable laws impacting the District;
3. limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
4. not use the PII for any purpose not explicitly authorized in its contract;
5. not disclose any PII to any other party without the prior written consent of the parent or eligible student:
    a. except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or
    b. unless required by statute or court order and the third-party contractor provides notice of disclosure to the District, unless expressly prohibited.
6. maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;
7. use encryption to protect PII in its custody; and
8. 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 immediately notify the District in the most expedient way possible without unreasonable delay, but no more than forty-eight (48) hours 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. This plan must be accepted by the District.

At a minimum, each plan will:

1. 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;
2. specify the safeguards and practices it has in place to protect PII;
3. demonstrate that it complies with the requirements of Section 121.3(c) of the Regulations of the Commissioner;
4. specify how those who have access to the student, teacher, or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
5. specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;
6. specify how the third-party contractor will manage data security and privacy incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;
7. 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

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

E. Reporting

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

F. Notifications

The Data Protection 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 ten (10) calendar days after such discovery, using a form or format prescribed by the New York State Education Department (NYSED).

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 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 and/or his/her designee, 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, teacher or principal PII.

"Private Information" under State Technology Law §208

Private information is defined in State Technology Law §208 and includes certain types of information 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 consultation 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.

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:

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

6. drivers' license number.

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

1. publicly posted or displayed;
2. visibly printed on any ID badge, card, or time card;
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: 1120, District Records
5500, Student Records

Ref: State Technology Law §§201-208
Labor Law §203-d
Education Law §§2-d; 3012-c
8 NYCRR Part 121
Family Educational Rights and Privacy Act, as amended, 20 USC §1232g
34 CFR Part 99

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