PARENTS BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY

Pursuant to Section 2-c and 2-d of the Education Law, parents and students are entitled to certain protections regarding confidential student information. The Poughkeepsie City School District is committed to safeguarding personally identifiable information from unauthorized access or disclosure as set forth below:

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;

3. The District is committed to implementing safeguards associated with industry standards and best practice under state and federal laws protecting the confidentiality of personally identifiable information, including but not limited to, encryption, firewalls, and password protection when data is stored or transferred;

4. A complete list of all student data elements collected by the State is available for public review at http://www.p12.nysed.gov/irs/vendors/templates.html or by writing to Information & Reporting Services, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234; and

5. Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed to the Assistant Superintendent of Assistant Superintendent for Data Analysis and Accountability at 11 College Avenue, Poughkeepsie, NY 12603.

6. The District has, directly and indirectly entered into contracts with certain third party contractors who have been sent student data and/or teacher data and/or principal data. The following information about such contractors will be posted on the District website, as required by law:

    - The names of the third party contractors, the exclusive purpose(s) for which the data will be used;
    - The commencement and termination dates of each such agreement;
    - A description of how the data will be disposed by the contractor when the contract purpose has been fulfilled;
    - The data storage and security measures undertaken.

7. Agreements with third party contractors/consultants will ensure that the subcontractors, persons or entities that the third party contractor/consultant will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements.

8. A parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected by filing a written request with the Superintendent of Schools or his/her administrative designee, the Assistant Superintendent for Data Analysis and Accountability at 11 College Avenue, Poughkeepsie, NY 12603.

Adopted: Jan. 16, 2019

INFORMATION SECURITY BREACH POLICY

I. This policy is consistent with Section 208 of the New York State Technology Law. School districts are required to notify any New York State resident 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 this policy.

II.

a.

i. The definition of "private information" shall mean personal information in combination with any one or more of the following data elements, when either (1) the personal information or the data element is not encrypted or (2) encrypted with a corresponding encryption key that has also been acquired:

1. Social Security Number.
2. Driver's license number or non-driver identification card number; or
3. Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

b. Private Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local governmental records.

c. This policy also applies to information maintained on behalf of a District by a third party.

III. Notification:

a. The District shall notify an individual when it has been determined that there has been, or is reasonably believed to have been a compromise of private information through unauthorized disclosure.

b. The District will notify the affected individual. Such notice shall be directly provided to the affected persons by one of the following methods:

i. written notice;
ii. electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the District who notifies affected persons in such form;
iii. telephone notification provided that a log of each such notification is kept by the District who notifies affected persons; or

iv. Substitute notice, if a District demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such District does not have sufficient contact information. Substitute notice shall consist of all of the following:

1. e-mail notice when such District has an e-mail address for the subject persons;
2. conspicuous posting of the notice on such District's web site page, if such District maintains one; and
3. notification to major statewide media.

c. The notice must include the District's contact information, a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which elements of private information were, or are reasonably believed to have been, so acquired.

d. Notification may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required shall be made after such law enforcement agency determines that such notification does not comprise such investigation.

IV. When notification is necessary, the District must also notify the following agencies as to the timing, content and distribution of the notices and approximate number of affected persons:

a. NYS Attorney General

b. NYS Office of Cyber Security & Critical Infrastructure Coordination

c. Consumer Protection Board

d. Consumer Reporting Agencies (ONLY if more than 5,000 New York State residents are notified at one time.)

Legal Ref: NYS General Business Law §899-aa; NYS Technology Law §208.

Adopted: Jan. 16, 2019