SECURITY BREACH AND NOTIFICATION

The Board of Education is committed to protecting the private information of Rochester City School District students, staff, and residents in the District's possession. The District's information systems are protected by advanced next generation firewall protection, end-point security, and email scanning. However, the evolving nature of technology and the potential gain from compromising information systems prevents any system from being absolutely inviolable. Should the District's records be compromised or private information be acquired without authorization, the District shall comply with the Information Security Breach and Notification Act and this policy.

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 data security and protection. The District's systems will at a minimum 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 District 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.

Definitions

Personal Information: any information concerning a natural person which, because of name, number, symbol, mark or other identifier, can be used to identify that natural person.

Private Information: personal information, which is not encrypted, which includes one or more of the following:

1. social security number;

2. driver's license number or non-driver identification card number;

3. home address, telephone number, personal electronic email address, user identification numbers or passwords to personal electronic accounts; or

4. account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an employee's or a student's personal information, employment records, academic records, or financial account.

Under Title I of the Elementary and Secondary Education Act, the District is required to provide student directory information to recruiters from colleges, prospective employers, and the military services. Parents must notify the District if they do not want their child's directory information to be shared with recruiters. (See the Recruiting by Organizations with Restrictive Membership or Employment Practices Authorized and Permitted by Law policy (1240.1) for more information). Student directory information includes: a student's address, telephone number, date and place of birth, name of last school attended, dates of attendance, field of study, and participation in athletic and extracurricular activities.

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

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

1. the protections of "personally identifiable information" of student and teachers/principal under Education Law §2-d and Part 121 of the Commissioner of Education;

2. the protections of "private information" under State Technology Law §208 and the NY SHIELD Act; and

3. procedures to notify persons affected by breaches or unauthorized access of protected information.

Breach of the Security of the System: unauthorized acquisition of computerized data which compromises the security, confidentiality, or integrity of personal information. Good faith acquisition of personal information by an employee or agent of a state entity for the purposes of the agency is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

The Superintendent shall establish regulations regarding the procedures to be used to:

1. identify any breaches of security that result in the release of private information;

2. ensure training is provided to District employees on an ongoing basis regarding information technology security awareness; and

3. inform the Chief of Communications Officer, who is responsible for notifying all individuals affected by the security breach.

Notification of Breach

The District's Chief of Communications Officer or designee shall notify affected persons of any breach of the security of its computer system(s) following discovery. Affected persons shall include all individuals whose private information was, or is reasonably believed to have been, acquired without valid authorization. The disclosure shall be made in the most expedient time possible, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The District's Chief of Communications Officer shall provide all notice required by this policy and shall include contact information at the District in order to respond to questions regarding the breach and a description of the categories of information that were, or are reasonably believed to have been, acquired without authorization. The Chief of Communications Officer shall provide such notice directly to the affected persons by one of the following methods:

1. written notice;

2. electronic notice; or

3. telephone notification.

Notice must be provided in a manner reasonably expected to be received by the affected persons. The District must maintain a log of all persons notified under this policy.

The Chief of Communications Officer shall also provide notice of any breach, its timing, and the approximate number of affected persons to the New York State Attorney General, the New York State Consumer Protection Board, and the New York State Office of Cyber Security and Critical Infrastructure.

In the event that more than five thousand New York residents are to be notified at one time, the District shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons.

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:

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 (i.e., students who are eighteen years old or older):

    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 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.

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 this Part;

4. 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;

5. 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;

6. 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;

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.

Cross-ref: School District Records (1120)
Media Relations (1130)
Recruiting by Organizations with Restrictive Membership or Employment Practices Authorized and Permitted by Law (1240.1)
Internet Policy (4526)

Ref: State Technology Law §§201-208
Labor Law §203-d

Notes: Adopted June 22, 2011 pursuant to Resolution No. 2010-11: 906; Amended July 26, 2018 pursuant to Resolution No. 2018-19: 80; Amended October 20, 2022 pursuant to Resolution No. 2022-23: 206

ct