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.

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.

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

Notification of Breach

The District's Chief 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 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 Communications Officer shall provide such notice directly to the affected persons by one of the following methods:

(a) written notice;

(b) electronic notice; or

(c) 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 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.

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

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

Adopted June 22, 2011 pursuant to Resolution No. 2010-11: 906; Amended July 26, 2018 pursuant to Resolution No. 2018-19: 80.