

## INFORMATION SECURITY BREACH AND NOTIFICATION

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. To this end, 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, which will include all “personally identifiable information” of students, and District employees under Education Law §2-d and Part 121 of the regulations of the Commissioner of Education. For purposes of this policy, “private information” does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;
- 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.

Additionally, pursuant to Labor Law §203-d, the district will not communicate employee “personal identifying information” to the general public. This includes but is not limited to social security number, home address or telephone number, personal email address, Internet identification name or password, parent’s surname prior to marriage, or driver’s license number. In addition, the district will protect employee social security numbers in that such numbers shall not: be publicly posted or displayed, be printed on any ID badge, card or time card, be placed in files with unrestricted access, or be used for occupational licensing purposes. Employees with access to such information shall be notified of these prohibitions and their obligations.

Any breach of the district’s information storage or computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the district shall be promptly reported to the Data Protection Officer, the Superintendent and the Board of Education.

Cross-ref:      1111, Public Access to School District Records  
                      1310, Release of Information about Staff Members, School Volunteers and Students  
                      3802, Technology Security for Personal, Private and Sensitive Information  
                      4410, Technology Acceptable Use Policy  
                      4411, Remote Access to Computer Network  
                      4420, Computer Controls Policy for Financial Software  
                      5125, Availability of Student Records in Accordance with the Family Educational Rights and Privacy Act of 1974  
                      6147, Technology Acceptable Use Policy (Students)

**Information Security Breach and Notification (Continued)**

Ref: State Technology Law  
§§201-208 Labor Law  
§203-d  
Education Law 2-d

Adoption date:

August 21, 2014

Reviewed:

October 24, 2016

Reviewed:

August 28, 2017

Reviewed:

August 27, 2018

Revised:

June 29, 2020

Reviewed:

October 24, 2022

Revised:

August 21, 2023

Revised:

September 16, 2024