Non-Instructional/Business Operations

**SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION**

The Board of Education acknowledges the State's concern regarding the rise in identity theft and the need for 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. 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 social security number, home address or telephone number, personal electronic 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 computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the district shall be promptly reported to the Superintendent and the Board of Education.

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

Note: Policy #7243 Student Data Breaches

First Reading: July 19, 2016
Adoption: September 8, 2016