Policy 8635

(X) Required
(X) Local
(X) Notice

INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION

The School District maintains students', teachers' and principals' private information, personally identifiable information, and education records on data management systems and recognizes its responsibility to protect the privacy of student data, including personally identifiable information, and its obligation to notify students and their parents, teachers and principals when a data security breach has/may have resulted in the unauthorized disclosure of, or access to, this information. Therefore, the School District has implemented privacy and security measures designed to protect student data stored in its student data management systems. These measures include reviewing information systems to identify where personally identifiable information is stored and used, and monitoring data systems to protect against and detect potential breaches. In the event of a breach or suspected breach, the School District will promptly take steps to validate the breach, mitigate any loss or damage, and notify law enforcement, if necessary.

To this end, the Superintendent of Schools or his/her designee, in accordance with appropriate business and technology personnel, will:

- 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 School District will not communicate employee and student "personally 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 School 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.

If the School District determines that a security breach has occurred, affected individuals will be provided notice without unreasonable delay. The notification method may vary depending on the type of data breached and the number of individuals affected and the Superintendent will be responsible for implementing an appropriate response. To this end, the Superintendent of Schools or his/her designee, in accordance with appropriate business and technology personnel, will:

- 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;

Any breach of the School District's computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the School District shall be promptly reported to the Superintendent of Schools and the Board of Education.

Definitions

"Private information" shall mean personal information (i.e., information such as name, number, symbol, mark or other identifier which can be used to identify a person) in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- Social security number;
- Driver's license number or non-driver identification card number; or
- 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; or
- Biometric information (data generated by electronic measurements of a person's physical characteristics, such as fingerprint, voice print, retina image or iris image) used to authenticate or ascertain a person's identity.

Note: "Private information" does not include publicly available information that is lawfully made available to the general public pursuant to state or federal law or regulation.

"Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the School District. Good faith acquisition of personal information by an officer or employee or agent of the School District for the purposes of the School District is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.

To successfully implement this policy, the School District shall inventory its computer programs and electronic files to determine the types of personal, private information that is maintained or used by the School District and review the safeguards in effect to secure and protect that information.

Ref: State Technology Law §§201-208
Labor Law §203-d
8 NYCRR Part 121

Adopted: September 15, 2010
Revised: May 12, 2021