SUBJECT: STUDENT DATA BREACHES

A student data breach is defined as any instance in which there is an unauthorized release of or access to personally identifiable information (PII) or other protected information of students not suitable for public release.

School districts have a legal responsibility to protect the privacy of education data, including personally identifiable information (PII) of its students. The Family Education Rights and Privacy Act of 1974, commonly known as FERPA, protects the privacy of student education records. Although FERPA does not include specific data breach notification requirements, it does protect the confidentiality of education records and requires districts to record each incident of data disclosure in accordance with 34 CFR 99.32 (a)(1). In addition, under state law, direct notification of parents and/or affected students may be warranted depending on the type of data compromised, such as student social security numbers and/or other identifying information that could lead to identity theft.

The 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 and data to indentify where personally identifiable information is stored and used; monitoring data systems to detect potential breaches; and conducting privacy and security awareness training for appropriate staff. In the event of an alleged breach, the District will promptly take steps to validate the breach, mitigate any loss or damage, and notify law enforcement if necessary.

The Superintendent will develop and implement regulations for prevention, response and notification regarding student data breaches.

34 CFR 99.32 (a)(1)
Technology Law Sections 202 and 208

NOTE: Refer also to Policies #5672 -- Information Security Breach and Notification
#7240 -- Student Records: Access and Challenge

Adopted by the Canaseraga Board of Education June 27, 2013