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 Ogdensburg City 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 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 Ogdensburg City School 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. A Parents' Bill of Rights for Data Privacy and Security is attached to this policy.

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

Adoption Date: October 6, 2014

The NYS Education Department's
Education Law §2-d Bill of Rights for Data Privacy and Security

Parents and eligible students[1] can expect the following:

1. A student's personally identifiable information (PII)[2] cannot be sold or released for any commercial purpose.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency.

3. State and federal laws,[3] such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, that protect the confidentiality of a student's PII, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

4. A complete list of all student data elements collected by NYSED is available for public review at www.nysed.gov/data-privacy-security, and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

5. The right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints may be submitted to NYSED online at www.nysed.gov/data-privacy-security, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234, by email to privacy@nysed.gov, or by telephone at 518-474-0937.

6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

7. Educational agency workers that handle PII will receive training on applicable state and federal laws, the educational agency's policies, and safeguards associated with industry standards and best practices that protect PII.

8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

---

[1] "Parent" means a parent, legal guardian, or person in parental relation to a student. These rights may not apply to parents of eligible students defined as a student eighteen years or older. "Eligible Student" means a student 18 years and older.

[2] "Personally identifiable information," as applied to student data, means personally identifiable information as defined in section 99.3 of title thirty-four of the code of federal regulations implementing the family educational rights and privacy act, section twelve hundred thirty-two-g of title twenty of the United States code, and, as applied to teacher or principal data, means "personally identifying information" as such term is used in subdivision ten of section three thousand twelve-c of this chapter.

[3] Information about other state and federal laws that protect student data such as the Children's Online Privacy Protection Act, the Protection of Pupil Rights Amendment, and NY's Personal Privacy Protection Law can be found at http://www.nysed.gov/student-data-privacy/federal-laws-protect-student-data.