8625 PRIVACY AND SECURITY FOR STUDENT, TEACHER AND PRINCIPAL DATA

The Board of Education recognizes its responsibility to enact policies that provide privacy for student, teacher and principal data in accordance with law. This is particularly relevant in the context of the administration of student data which is collected, surveys that collect personal information, the disclosure of personal information for marketing purposes and in conducting physical exams.

As provided in Education Law Section 2-d and/or its implementing regulations, the following terms, as used in this policy, will mean:

a) "Breach" means the unauthorized acquisition, access, use, or disclosure of student data and/or teacher or principal data by or to a person not authorized to acquire, access, use, or receive the student data and/or teacher or principal data.

b) "Building principal" means a building principal subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

c) "Classroom teacher" means a teacher subject to annual performance evaluation review under the provisions of Education Law Section 3012-c.

d) "Commercial or marketing purpose" means the sale of student data; or its use or disclosure for purposes of receiving remuneration, whether directly or indirectly; the use of student data for advertising purposes, or to develop, improve, or market products or services to students.

e) "Contract or other written agreement" means a binding agreement between an educational agency and a third-party, which includes, but is not limited to, an agreement created in electronic form and signed with an electronic or digital signature or a click-wrap agreement that is used with software licenses, downloaded, and/or online applications and transactions for educational technologies and other technologies in which a user must agree to terms and conditions prior to using the product or service.

f) "Disclose" or "disclosure" means to permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written, or electronic, whether intended or unintended.

g) "Education records" means an education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

h) "Educational agency" means a school district, board of cooperative educational services (BOCES), school, or the New York State Education Department (NYSED).

i) "Eligible student" means a student who is eighteen years or older.

j) "Encryption" means methods of rendering personally identifiable information unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified or permitted by the Secretary of the United States Department of Health and Human Services in guidance issued under 42 USC Section 17932(h)(2).

k) "FERPA" means the Family Educational Rights and Privacy Act and its implementing regulations, 20 USC Section 1232g and 34 CFR Part 99, respectively.

l) "NIST Cybersecurity Framework" means the U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). A copy of the NIST Cybersecurity Framework is available at the Office of Counsel, State Education Department, State Education Building, Room 148, 89 Washington Avenue, Albany, New York 12234.

m) "Parent" means a parent, legal guardian, or person in parental relation to a student.

n) "Personally identifiable information (PII)," as applied to student data, means personally identifiable information as defined in 34 CFR Section 99.3 implementing the Family Educational Rights and Privacy Act, 20 USC Section 1232g, and, as applied to teacher or principal data, means personally identifying information as this term is defined in Education Law Section 3012-c(10).

o) "Release" has the same meaning as disclosure or disclose.

p) "Student" means any person attending or seeking to enroll in an educational agency.

q) "Student data" means personally identifiable information from the student records of an educational agency.

r) "Teacher or principal data" means personally identifiable information from the records of an educational agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law Sections 3012-c and 3012-d.

s) "Third-party contractor" means any person or entity, other than an educational agency, that receives student data or teacher or principal data from an educational agency pursuant to a contract or other written agreement for purposes of providing services to the educational agency, including but not limited to data management or storage services, conducting studies for or on behalf of the educational agency, or audit or evaluation of publicly funded programs. This term will include an educational partnership organization that receives student and/or teacher or principal data from a school district to carry out its responsibilities pursuant to Education Law Section 211-e and is not an educational agency, and a not-for-profit corporation or other nonprofit organization, other than an educational agency.

t) "Unauthorized disclosure" or "unauthorized release" means any disclosure or release not permitted by federal or state statute or regulation, any lawful contract or written agreement, or that does not respond to a lawful order of a court or tribunal or other lawful order.

District Data Privacy and Security Standards

The School District will use the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1) (Framework) as the standard for its data privacy and security program. The Framework is a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. The Framework provides a common taxonomy and mechanism for organizations to:

a) Describe their current cybersecurity posture;

b) Describe their target state for cybersecurity;

c) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;

d) Assess progress toward the target state; and

e) Communicate among internal and external stakeholders about cybersecurity risk.

The School District will protect the privacy of PII by:

a) Ensuring that every use and disclosure of PII by the District benefits students and the School District by considering, among other criteria, whether the use and/or disclosure will:

1. Improve academic achievement;
2. Empower parents and students with information; and/or
3. Advance efficient and effective school operations.

b) Not including PII in public reports or other public documents.

The School District affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

Data Protection Officer

The School District has designated a School District employee to serve as the School District's Data Protection Officer.

The Data Protection Officer is responsible for the implementation and oversight of this policy and any related procedures including those required by Education Law Section 2-d and its implementing regulations, as well as serving as the main point of contact for data privacy and security for the School District.

The School District will provide training to the Data Protection Officer to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities.

Data Collection Transparency and Restrictions

As part of its commitment to maintaining the privacy and security of student data and teacher and principal data, the School District will take steps to minimize its collection, processing, and transmission of PII. Additionally, the School District will:

a) Not sell PII nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so.

b) Ensure that it has provisions in its contracts with third-party contractors or in separate data sharing and confidentiality agreements that require the confidentiality of shared student data or teacher or principal data be maintained in accordance with law and School District policy.

Except as required by law or in the case of educational enrollment data, the School District will not report to NYSED the following

student data elements:

a) Juvenile delinquency records;

b) Criminal records;

c) Medical and health records; and

d) Student biometric information.

Nothing in Education Law Section 2-d or this policy should be construed as limiting the administrative use of student data or teacher or principal data by a person acting exclusively in the person's capacity as an employee of the School District.

Privacy and Security of Student Data

The Board of Education is committed to protecting the privacy and security of each and every student's data. In accordance with law, the following shall govern parental rights concerning their child's data:

1. A student's personally identifiable information cannot be sold or released for any commercial purposes.
2. Parents/guardians have the right to inspect and review the complete contents of their child's education record.
3. The confidentiality of a student's personally identifiable information is protected by existing state and federal laws, and safeguards such as encryption, firewalls, and password protection, must be in place when data is stored or transferred. Third party contractors are required to employ technology, safeguards and practices that align with the National Institute of Standards and Technology Cybersecurity Framework.
4. A complete list of all student data elements collected by the State Education Department is available for public review at:

   http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/collected-data-elements.pdf,

   or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, NY 12234.

5. Parents/guardians have the right to file complaints about possible breaches of student data. Parents/guardians may submit a complaint regarding a potential breach by the School District to the Superintendent of Schools or his/her designee. Complaints pertaining to the State Education Department or one of its third party vendors should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany NY 12234, email to privacy@nysed.gov. The complaint process is under development and will be established through regulations to be proposed by the State Education Department's Chief Privacy Officer.
6. In the event of a data breach or unauthorized disclosure of students' personally identifiable information, third party contractors are required by law to notify the School District within seven (7) days of discovery of the breach or unauthorized disclosure.
7. If the District enters into a contract in which student, teacher, or principal data is shared with a third party, the School District will require the contractor to provide evidence that it has adopted a data and security plan in accordance with Education Law, section 2-d and will post as supplemental information to be appended to the Parents' Bill of Rights the following information:
   a. the exclusive purposes for which the student data will be used;
   b. how the service provider will ensure that subcontractors, persons or entities that the service provider will share the student data with, if any, will abide by data protection and security requirements;
   c. that student data will be returned or destroyed upon expiration of the Agreement;
   d. if and how a parent, student, or eligible student may challenge the accuracy of the student data that is collected; and
   e. where the student data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.
8. Parents may access the State Education Department's Parents' Bill of Rights at: http://www.nysed.gov/common/nysed/files/programs/student-data-privacy/parents-bill-of-rights.pdf.
9. The School District will post a Parents' Bill of Rights in accordance with the requirements of Education Law.
10. The School District will designate a Data Protection Officer on an annual basis who shall be responsible for the implementation of policies and procedures required by law and to serve as the point of contact for data security and privacy for the School District.

The School District will publish on its website the supplement to the Bill of Rights (i.e., the supplemental information described above) for any contract or other written agreement it has entered into with a third-party contractor that will receive PII from the School District. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the School District's data and/or technology infrastructure.

The School District will maintain a record of all complaints of breaches or unauthorized releases of student data and their

disposition in accordance with applicable data retention policies, including the Records Retention and Disposition Schedule ED-1.

Third-Party Contractors

School District Responsibilities

The School District will ensure that whenever it enters into a contract or other written agreement with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the School District, the contract or written agreement will include provisions requiring that confidentiality of shared student data or teacher or principal data be maintained in accordance with law and School District policy.

In addition, the School District will ensure that the contract or written agreement includes the third-party contractor's data privacy and security plan that has been accepted by the School District.

Surveys

The Board of Education recognizes that student surveys are a valuable tool in determining student needs for educational services. In accordance with law and Board policy, parental consent is required for minors to take part in surveys which gather any of the following information:

1. political affiliations or beliefs of the student or the student's parent/guardian;
2. mental or psychological problems of the student or the student's family;
3. sex behavior or attitudes;
4. illegal, anti-social, self-incriminating or demeaning behavior;
5. critical appraisals of other individuals with whom respondents have close family relationships;
6. legally recognized privileged or analogous relationships, such as those of lawyers, physicians and ministers;
7. religious practices, affiliations or beliefs of the student or the student's parent/guardian; or
8. income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program).

In the event that the School District plans to survey students to gather information included in the list above, the School District will obtain written consent from the parent/guardian in advance of administering the survey. The notification/consent form will also apprise the parent/guardian of their right to inspect the survey prior to their child's participation.

Marketing

It is the policy of the Board of Education not to collect, disclose, or use personal information gathered from students for the purpose of marketing or selling that information or providing it to others for that purpose. "Personal Information" is defined as: "individually identifiable information concerning the student, including a student's or parent's first and last name, home address, telephone numbers and/or social security number." This does not apply to the collection, disclosure, or use of personal information collected from students for the exclusive purpose of developing, evaluating, or providing educational products or services for, or to students or educational institutions such as:

1. College or other postsecondary education recruitment, or military recruitment;
2. Book clubs, magazines and programs providing access to low-cost literary products;
3. Curriculum and instructional materials used in schools;
4. Tests and assessments used to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information for students or to generate other statistically useful data for the purpose of securing such tests and assessments, and the subsequent analysis and public release of the aggregate data from such tests and assessments;
5. Student recognition programs; and
6. The sale by students of products or services to raise funds for school-related activities.

In the event that such data is collected by the School District, disclosure or use of student personal information will be protected by the School District pursuant to the requirements of the Family Educational Rights and Privacy act (FERPA).

Inspection of Instructional Material

Parents/guardians shall have the right to inspect, upon request, any instructional material, used as part of the educational curriculum for students. "Instructional material" is defined as: "instructional content that is provided to a student, regardless of format including printed or representational materials, audio-visual materials, and materials in electronic or digital formats (such as materials accessible through the Internet). It does not include tests or academic assessments."

A parent/guardian who wishes to inspect and review such instructional material shall submit a request in writing to the Building

Principal. Upon receipt of such request, arrangements shall be made to provide access to such material to within thirty (30) calendar days after the request has been received.

Invasive Physical Examinations

Prior to the administration of any non-emergency, invasive physical examination or screening that is required as a condition of attendance, administered by the school not necessary to protect the immediate health or safety of the student or other students and not otherwise permitted or required by state law, a student's parent/guardian will be notified and given an opportunity to opt their child out of the exam. Hearing, vision and scoliosis screenings are not subject to prior notification. The term "invasive physical examination" means any medical examination that involves the exposure of private body parts, or any act during such examination that includes incision, insertion, or injecting into the body, but does not include a hearing, vision or scoliosis screening.

Notification of Rights

Parents/guardians and eligible students shall be notified of this policy at least annually, at the beginning of the school year and when enrolling students for the first time in the School District's schools. In the annual notification, the School District shall notify the parents/guardians and eligible students of the specific or approximate dates during the school year when the activities involving collection, disclosure or use of personal information collected from students for the purpose of marketing or selling the information, administration of any surveys, and any non-emergency, invasive physical exams or screenings, are scheduled or expected to be scheduled. The annual notification shall also inform parents/guardians and eligible students that, upon request, the School District will disclose the name, address and telephone number of high school students to military recruiters and institutions of higher learning unless the parents/guardians or eligible students exercise their right to prohibit the release of the information without prior written consent. The School District shall also notify parents/guardians and eligible students within a reasonable period of time after any substantive change to this policy.

Notification of Breach or Unauthorized Release

The School District will notify affected parents, eligible students, teachers and/or principals of a breach or unauthorized release of information as set forth in Policy 8635, Information Security Breach and Notification.

Cross-ref:

8630 Computer Resources and Data Management

8635 Information Security Breach and Notification

Ref:

20 USC §1232h

34 CFR Part 98

Education Law, section 2-d; Education Law §903

8 NYCRR Part 121

Adoption date: September 10, 2020