SUBJECT: SPECIAL MEETINGS OF THE BOARD

Any member of the Board may call for a special meeting. A reasonable and good-faith effort will be made by the Superintendent or the Board president, as the case may be, to give every member of the Board 24-hours' notice of the time, place, and purpose of the meeting. In an emergency, however, the members may waive the 24-hour notice requirement.

All special meetings will be held at a regular meeting place of the Board and in accordance with all applicable provisions of the Open Meetings Law. Public notice of the time and place will be given, to the extent practicable, to the news media, and it will be conspicuously posted in one or more designated public locations at a reasonable time before the meeting.

Education Law § 1606(3)
Public Officers Law §§ 103 and 104

NOTE: Refer also to Policy #1510 -- Regular Board Meetings and Rules (Quorum and Parliamentary Procedure)

Adoption Date

SUBJECT: EXECUTIVE SESSIONS

Upon a majority vote of its total membership, taken in an open meeting in accordance with a motion identifying the general area or areas of the subject or subjects to be considered, the Board may conduct an executive session for discussion of the below listed purposes only, provided, however, that no action by formal vote will be taken except on an Education Law Section 3020-a probable cause finding. For all other purposes, the action by formal vote will be taken in open meeting and properly recorded in the minutes of the meeting. Attendance at an executive session will be permitted to any Board member and any persons authorized or requested to attend by the Board. The Superintendent will attend all executive sessions except those that concern his or her evaluation, employment, or salary.

a) Matters that will imperil the public safety if disclosed;

b) Any matter that may disclose the identity of a law enforcement agent or informer;

c) Information relating to current or future investigation or prosecution of a criminal offense that would imperil effective law enforcement if disclosed;

d) Discussions regarding proposed, pending or current litigation;

e) Collective negotiations pursuant to Civil Service Law Article 14;

f) Medical, financial, credit, or employment history of any particular person or corporation, or matters leading to the appointment, employment, promotion, demotion, discipline, suspension, dismissal or removal of any particular person or corporation;

g) Preparation, grading, or administration of examinations;

h) Proposed acquisition, sale, or lease of real property or the proposed acquisition of securities, or sale or exchange of securities, but only when publicity would substantially affect the value.

Motions for executive sessions should state the subject or subjects to be discussed in executive session. It is insufficient to merely recite statutory language.

Matters discussed in executive sessions must be treated as confidential.

Education Law §§ 1708(3) and 3020-a
Public Officers Law Article 7

Adoption Date

SUBJECT: DIVERSITY, EQUITY, AND INCLUSION IN THE DISTRICT*

Overview

Research shows that all students benefit when schools implement strong diversity, equity, and inclusion (DEI) policies and practices. These benefits include academic, cognitive, civic, social-emotional, and economic. This is true regardless of a school's geographic location or the demographic composition of its students and staff.

This policy provides a framework as to how the District will foster DEI in its schools. This policy considers the entirety of the educational process by addressing the following essential elements: governance; teaching and learning; family and community engagement; workforce diversity; diverse schools and learning opportunities; and student supports, discipline, and wellness. It is just one component of the District's overall commitment to maintaining a diverse, equitable, and inclusive educational and work environment.

**The District may develop a DEI plan to manage and coordinate the execution of this policy.

***Inquiries about this policy may be directed to the District's DEI Coordinator.

Defining Diversity, Equity, and Inclusion

For purposes of this policy:

a) "Diversity" includes, but is not limited to: race; color; ethnicity; nationality; religion; socioeconomic status; veteran status; education; marital status; language; age; gender; gender expression; gender identity; sexual orientation; mental or physical ability; genetic information; and learning style.

b) "Equity" includes, but is not limited to, seeking the fair treatment, access, opportunity, and advancement for all while striving to identify and eliminate barriers that have prevented the full participation of all groups.

**Customize to District -- This sample policy is based on the policy statement on DEI issued by the NYS Board of Regents. It should be reviewed and customized by your District as appropriate for its specific circumstances and practices. It is recommended that districts keep the language in this policy high-level and that implementation details be placed in procedural documents.*
***Customize to District -- A DEI plan is one way by which a district may choose to manage and coordinate the execution of this policy. It is not a required document. If your District does not plan on developing and maintaining a DEI plan, it should delete this sentence.*
****Customize to District -- If your District does not designate a DEI Coordinator, this sentence should be deleted or modified.*

(Continued)

SUBJECT: DIVERSITY, EQUITY, AND INCLUSION IN THE DISTRICT (Cont'd.)

c) "Inclusion" includes, but is not limited to, authentically bringing traditionally excluded individuals and/or groups into processes, activities, and decision/policy making in a way that shares power and ensures equal access to opportunities and resources.

These descriptions are not intended to be exhaustive. Rather, they are meant to be foundational and provide clarity to the concepts of diversity, equity, and inclusion.

Governance

DEI Committee

The District has established a DEI Committee that meets periodically throughout the year. The purpose of the DEI Committee is to assist the District in creating and implementing plans that advance the District's commitment to maintaining a diverse, equitable, and inclusive environment where all individuals feel valued and respected. As needed, the DEI Committee will also review District policies, practices, and programs and provide suggestions as to how they could potentially be modified to better promote DEI.

The District will actively seek members for the DEI Committee through the use of email, newsletters, the District's website, the District's social media page(s), and/or advertisements.

The DEI Committee will be representative of all stakeholders, and may include (to the extent possible), but not be limited to, representatives from the following groups:

a) Students;

b) Parents and persons in parental relation;

c) District/building administrators;

d) Teachers, including at least one special education teacher;

e) Guidance staff, including at least one school psychologist, social worker, or counselor;

f) Other District staff;

g) The Board; and

h) Community members.

(Continued)

SUBJECT: DIVERSITY, EQUITY, AND INCLUSION IN THE DISTRICT (Cont'd.)

*DEI Coordinator

The Superintendent has designated the following District employee to serve as its DEI Coordinator:

[*For the DEI Coordinator, the District should list the following: name or title, office address, telephone number, and email address.*]

The DEI Coordinator will be a member of the DEI Committee and convene and coordinate the activities and plans of the DEI Committee.

Teaching and Learning

The District will strive to advance inclusive and culturally responsive teaching and learning through, but not limited to, the following means: curricula in all content areas; books and instructional materials; pedagogical practices and professional development; classroom grouping policies and practices; student support systems for all developmental pathways; full and equitable opportunities to learn for all students; and multiple assessment measures. As part of this effort, the District will seek to:

a) Implement a Culturally Responsive-Sustaining (CR-S) Education Framework that embeds the ideals of diversity, equity, and inclusion by creating student-centered learning environments that:

1. Affirm cultural identities;
2. Foster positive academic outcomes;
3. Develop students' abilities to connect across lines of difference;
4. Elevate historically marginalized voices;
5. Empower students as agents of social change; and
6. Contribute to individual student engagement, learning, growth, and achievement through the cultivation of critical thinking.

b) Develop curricula that incorporates diverse perspectives, materials, and texts so that students are taught topics not just from one single perspective, but from multiple perspectives.

**Customize to District -- Designating a DEI Coordinator is one way by which a district may choose to organize its DEI Committee. There is no requirement that districts designate a DEI Coordinator. If your District does not plan on designating a DEI Coordinator, it should delete the "DEI Coordinator" subsection.*

(Continued)

SUBJECT: DIVERSITY, EQUITY, AND INCLUSION IN THE DISTRICT (Cont'd.)

c) Offer coherent opportunities for students to actively participate in experiences that prepare them for a lifetime of civic engagement and contributions to social justice, including, for example, completing projects that enable them to apply the learning they have acquired within and across subject areas.

d) Encourage academic discussions about racism and bigotry.

Family and Community Engagement

The District will strive to foster family and community engagement practices that are based on mutual trust, confidence, and respect. As part of this effort, the District will seek to:

a) Encourage participation from all stakeholders in community building conversations.

b) Reduce language barriers through various means, including, but not limited to, providing translated communications when appropriate.

c) Leverage partners such as the county government and local community organizations in developing DEI programs and activities for the District.

Workforce Diversity

The District will strive to create a workforce that is not only diverse and inclusive, but one that recognizes and values the differences among people. As part of this effort, the District will seek to:

a) Recruit and retain a diverse workforce in all areas and at all levels, thereby reducing stereotypes and preparing students for an increasingly global society.

b) Provide staff with opportunities for professional development on cultural proficiency.

Diverse Schools and Learning Opportunities

The District will strive to promote diverse, equitable, and inclusive classrooms in which students have equal access and opportunities to learn and realize their full potential. As part of this effort, the District will seek to:

a) Take creative steps to enhance the level of socioeconomic and racial diversity within District schools.

b) Eliminate the use of terms and phrases within District schools that perpetuate negative stereotypes and minimize student opportunities.

(Continued)

SUBJECT: DIVERSITY, EQUITY, AND INCLUSION IN THE DISTRICT (Cont'd.)

c) Create coursework, programs, and activities that are accessible to all students, regardless of their disability status, native language, income level, or any other basis.

Student Supports, Discipline, and Wellness

The District will strive to focus on the well-being of the "whole child." As part of this effort, the District will seek to:

a) Employ programs and practices that enhance all students' self-identity, self-confidence, and self-esteem.

b) Maintain non-discriminatory discipline policies and practices.

c) Consider and address the full range of student developmental pathways.

Training

To foster DEI in its schools, the District will provide DEI training to staff and students, as appropriate. This training may be delivered in various forms including, but not limited to: workshops; instructor-led classes; webinars; videos; workbooks; pamphlets; and/or emailed information. Although specific objectives will vary from training to training, in general, trainings will be designed to:

a) Increase awareness of the content of this policy and/or various DEI issues; and

b) Promote a welcoming and inclusive environment for all District community members.

Special trainings may be provided to members of the DEI Committee.

Notification

The District will share information about this policy via the District website and/or District-wide communications, as appropriate.

NOTE: Refer also to Policy #8241 -- Patriotism, Citizenship, and Human Rights Education

Adoption Date

SUBJECT: MEAL CHARGING AND PROHIBITION AGAINST MEAL SHAMING

[Districts participating in the National School Lunch Program and/or School Breakfast Program must adopt a policy addressing meal charging and prohibiting meal shaming. The policy is not needed where there is District-wide participation in the Community Eligibility Provision (CEP) or Provision 2, but is needed if only some, but not all schools within a district participate in CEP or Provision 2.]

It is the District's goal to provide students with access to nutritious no- or low-cost meals each school day and to ensure that a student whose parent/guardian has unpaid meal charges is not shamed or treated differently than a student whose parent/guardian does not have unpaid meal charges.

Unpaid meal charges place a large financial burden on the District. The purpose of this policy is to ensure compliance with federal requirements for the USDA Child Nutrition Program and to provide oversight and accountability for the collection of outstanding student meal balances to ensure that the student is not stigmatized, distressed, or embarrassed.

The intent of this policy is to establish procedures to address unpaid meal charges throughout the District in a way that does not stigmatize, distress, or embarrass students. The provisions of this policy pertain to regular priced reimbursable school breakfast, lunch and snack meals only. Charging of items outside of the reimbursable meals (a la carte items, adult meals, etc.) is expressly prohibited.

Access to Meals

a) Free meal benefit eligible students will be allowed to receive a free breakfast and lunch meal of their choice each day. A la carte items or other similar items must be paid/prepaid.

b) Reduced meal benefit eligible students will be allowed to receive a breakfast of their choice for $0.00 and lunch of their choice for $0.00 each day. A la carte items or other similar items must be paid/prepaid.

c) Full pay students will pay for meals at the District's published paid meal rate each day. The charge meals offered to students will be reimbursable meals available to all students, unless the student's parent or guardian has specifically provided written permission to the District to withhold a meal. A la carte items or other similar items must be paid/prepaid.

Ongoing Staff Training

a) Staff will be trained annually and throughout the year as needed on the procedures for managing meal charges using the State Education Department (SED) Webinar or the District's training program.

(Continued)

SUBJECT: MEAL CHARGING AND PROHIBITION AGAINST MEAL SHAMING (Cont'd.)

b) Staff training will include ongoing eligibility certification for free or reduced-price meals.

Parent Notification

Parents/guardians will be notified that a student's meal card or account balance is exhausted and has accrued unpaid meal charges within *[*enter number*] days of the charge and then every *[*enter number*] days/weeks thereafter.

Parent Outreach

a) Staff will communicate with parents/guardians with five or more unpaid meal charges to determine eligibility for free or reduced-price meals.

b) Staff will make two documented attempts to reach out to parents/guardians to complete a meal application in addition to the application and instructions provided in the school enrollment packet.

c) Staff will contact the parent/guardian to offer assistance with completion of meal application to determine if there are other issues within the household causing the student to have insufficient funds, offering any other assistance that is appropriate.

Minimizing Student Distress

a) Staff will not publicly identify or stigmatize any student in line for a meal or discuss any outstanding meal debt in the presence of any other students.

b) Students with unpaid meal charges will not be required to wear a wristband or handstamp, or to do chores or other work to pay for meals.

c) Staff will not throw away a meal after it has been served because of the student's inability to pay for the meal or because of previous unpaid meal charges.

d) Staff will not take any action directed at a student to collect unpaid meal charges.

e) Staff will deal directly with parents/guardians regarding unpaid meal charges.

Ongoing Eligibility Certification

a) Staff will conduct direct certification through the New York Student Identification System (NYSSIS) or using SED Roster Upload to maximize free eligibility. NYSED provides updated direct certification data monthly.

**Customize to District*

(Continued)

SUBJECT: MEAL CHARGING AND PROHIBITION AGAINST MEAL SHAMING (Cont'd.)

b) Staff will provide parents/guardians with free and reduced-price application and instructions at the beginning of each school year in the school enrollment packet.

c) If the District uses an electronic meal application, it will provide an explanation of the process in the school enrollment packet and instructions on how to request a paper application at no cost.

d) The District will provide at least two additional free and reduced-price applications throughout the school year to families identified as owing meal charges.

e) The District will use its administrative prerogative to complete an application on a student's behalf judiciously, and only after using exhaustive efforts to obtain a completed application from the student's parent/guardian. The District will complete the application using only available information on family size and income that falls within approvable guidelines.

f) The District will coordinate with the foster, homeless, migrant, and runaway coordinators to certify eligible students. School liaisons required for homeless, foster, and migrant students will coordinate with the nutrition department to make sure these students receive free school meals, in accordance with federal law.

Prepaid Accounts

Students/Parents/Guardians may pay for meals in advance via *[*web address for prepay*] or with a check payable to *[*lunch fund name*]. Further details are available on the District's webpage at *[*District web address*]. Funds should be maintained in accounts to minimize the possibility that a student may be without meal money on any given day. Any remaining funds for a particular student *[*may/will*] be carried over to the next school year.

To obtain a refund for a withdrawn or graduating student, a written or e-mailed request for a refund of any money remaining in the student's account must be submitted. Students who are graduating at the end of the year will be given the option to transfer any remaining money to a sibling's account through a written request.

Unclaimed funds must be requested within one school year. Unclaimed funds will then become the property of the District Food Service Program.

42 USC § 1758
7 CFR §§ 210.12 and 245.5
Education Law § 908
8 NYCRR § 114.5

**Customize to District*
Adoption Date

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION

The District values the protection of private information of individuals in accordance with applicable law and regulations. The District is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the individual's private information in compliance with the Information Security Breach and Notification Act and Board policy.

a) "Personal information" means any information concerning a person which, because of name, number, symbol, mark, or other identifier, can be used to identify that person.

b) "Private information" means either:

1. Personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

   (a) Social security number;

   (b) Driver's license number or non-driver identification card number;

   (c) Account number, credit or debit card number, in combination with any required security code, access code, password, or other information which would permit access to an individual's financial account;

   (d) Account number, or credit or debit card number, if circumstances exist where the number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or

   (e) Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation which are used to authenticate or ascertain the individual's identity;

2. A username or email address in combination with a password or security question and answer that would permit access to an online account.

Private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

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

Determining if a Breach Has Occurred

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or person without valid authorization, the District may consider the following factors, among others:

a) Indications that the information is in the physical possession or control of an unauthorized person, such as a lost or stolen computer or other device containing information;

b) Indications that the information has been downloaded or copied;

c) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or

d) System failures.

Notification Requirements

a) For any computerized data owned or licensed by the District that includes private information, the District will disclose any breach of the security of the system following discovery or notification of the breach to any New York State resident whose private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization. The disclosure to affected individuals will be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach and restore the integrity of the data system. The District will consult with the New York State Office of Information Technology Services to determine the scope of the breach and restoration measures. Within 90 days of the notice of the breach, the New York State Office of Information Technology Services will deliver a report to the District on the scope of the breach and recommendations to restore and improve the security of the system.

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

b) Notice to affected persons under State Technology Law is not required if the exposure of private information was an inadvertent disclosure by persons authorized to access private information, and the District reasonably determines the exposure will not likely result in the misuse of the information, or financial or emotional harm to the affected persons. This determination must be documented in writing and maintained for at least five years. If the incident affected over 500 New York State residents, the District will provide the written determination to the New York State Attorney General within ten days after the determination.

c) If notice of the breach of the security of the system is made to affected persons pursuant to the breach notification requirements under certain laws and regulations, the District is not required to provide additional notice to those affected persons under State Technology Law. However, the District will still provide notice to the New York State Attorney General, the New York State Department of State, the New York State Office of Information Technology Services, and to consumer reporting agencies.

d) For any computerized data maintained by the District that includes private information which the District does not own, the District will notify the owner or licensee of the information of any breach of the security of the system immediately following discovery, if the private information was, or is reasonably believed to have been, accessed or acquired by a person without valid authorization.

The notification requirement may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The required notification will be made after the law enforcement agency determines that the notification does not compromise the investigation.

If the District is required to provide notification of a breach, including breach of information that is not private information, to the United States Secretary of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act, it will provide notification to the New York State Attorney General within five business days of notifying the United States Secretary of Health and Human Services.

Methods of Notification

The required notice will be directly provided to the affected persons by one of the following methods:

a) Written notice;

b) Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form and a log of each notification is kept by the District when notifying affected persons in electronic form. However, in no case will the District require a person to consent to accepting the notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

(Continued)

SUBJECT: INFORMATION SECURITY BREACH AND NOTIFICATION (Cont'd.)

c) Telephone notification, provided that a log of each notification is kept by the District when notifying affected persons by phone; or

d) Substitute notice, if the District demonstrates to the New York State Attorney General that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or that the District does not have sufficient contact information. Substitute notice will consist of all of the following:

1. Email notice when the District has an email address for the subject persons;

2. Conspicuous posting of the notice on the District's website page, if the District maintains one; and

3. Notification to major statewide media.

Regardless of the method by which notice is provided, the notice will include:

a) Contact information for the notifying District;

b) The telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information; and

c) A description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, accessed or acquired.

In the event that any New York State residents are to be notified, the District will notify the New York State Attorney General, New York State Department of State, and New York State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons and provide a copy of the template of the notice sent to affected persons. This notice will be made without delaying notice to affected New York State residents.

In the event that more than 5,000 New York State residents are to be notified at one time, the District will also notify consumer reporting agencies as to the timing, content, and distribution of the notices and approximate number of affected persons. This notice will be made without delaying notice to affected New York State residents.

A list of consumer reporting agencies will be compiled by the New York State Attorney General and furnished upon request to any district required to make a notification in accordance with State Technology Law.

State Technology Law §§ 202 and 208
Adoption Date

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA

The District is committed to maintaining the privacy and security of student data and teacher and principal data and will follow all applicable laws and regulations for the handling and storage of this data in the District and when disclosing or releasing it to others, including, but not limited to, third-party contractors. The District adopts this policy to implement the requirements of Education Law Section 2-d and its implementing regulations, as well as to align the District's data privacy and security practices with the National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1).

Definitions

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.

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

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 18 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

(Continued)

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.

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 District will take steps to minimize its collection, processing, and transmission of PII. Additionally, the 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, regulation, and District policy.

Except as required by law or in the case of educational enrollment data, the 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 District.

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

Chief Privacy Officer

The Commissioner of Education has appointed a Chief Privacy Officer who will report to the Commissioner on matters affecting privacy and the security of student data and teacher and principal data. Among other functions, the Chief Privacy Officer is authorized to provide assistance to educational agencies within the state on minimum standards and best practices associated with privacy and the security of student data and teacher and principal data.

The District will comply with its obligation to report breaches or unauthorized releases of student data or teacher or principal data to the Chief Privacy Officer in accordance with Education Law Section 2-d, its implementing regulations, and this policy.

The Chief Privacy Officer has the power, among others, to:

a) Access all records, reports, audits, reviews, documents, papers, recommendations, and other materials maintained by the District that relate to student data or teacher or principal data, which includes, but is not limited to, records related to any technology product or service that will be utilized to store and/or process PII; and

b) Based upon a review of these records, require the District to act to ensure that PII is protected in accordance with laws and regulations, including but not limited to requiring the District to perform a privacy impact and security risk assessment.

Data Protection Officer

The District has designated a District employee to serve as the District's Data Protection Officer. *The Data Protection Officer for the District is:

_____

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 District.

The District will ensure that the Data Protection Officer has the appropriate knowledge, training, and experience to administer these functions. The Data Protection Officer may perform these functions in addition to other job responsibilities. Additionally, some aspects of this role may be outsourced to a provider such as a BOCES, to the extent available.

**Customize to District*

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

District Data Privacy and Security Standards

The 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 District will protect the privacy of PII by:

a) Ensuring that every use and disclosure of PII by the District benefits students and the 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 District affords all protections under FERPA and the Individuals with Disabilities Education Act and their implementing regulations to parents or eligible students, where applicable.

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

Third-Party Contractors

District Responsibilities

The 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 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, regulation, and District policy.

In addition, the 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 District.

The third-party contractor's data privacy and security plan must, at a minimum:

a) Outline how the third-party contractor will implement all state, federal, and local data privacy and security contract requirements over the life of the contract, consistent with District policy;

b) Specify the administrative, operational, and technical safeguards and practices the third-party contractor has in place to protect PII that it will receive under the contract;

c) Demonstrate that the third-party contractor complies with the requirements of 8 NYCRR Section 121.3(c);

d) Specify how officers or employees of the third-party contractor and its assignees who have access to student data or teacher or principal data receive or will receive training on the laws governing confidentiality of this data prior to receiving access;

e) Specify if the third-party contractor will utilize subcontractors and how it will manage those relationships and contracts to ensure PII is protected;

f) Specify how the third-party contractor will manage data privacy and security incidents that implicate PII including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the District;

g) Describe whether, how, and when data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires; and

h) Include a signed copy of the Parents' Bill of Rights for Data Privacy and Security.

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

Third-Party Contractor Responsibilities

Each third-party contractor, that enters into a contract or other written agreement with the District under which the third-party contractor will receive student data or teacher or principal data from the District, is required to:

a) Adopt technologies, safeguards, and practices that align with the NIST Cybersecurity Framework;

b) Comply with District policy and Education Law Section 2-d and its implementing regulations;

c) Limit internal access to PII to only those employees or subcontractors that have legitimate educational interests (i.e., they need access to provide the contracted services);

d) Not use the PII for any purpose not explicitly authorized in its contract;

e) Not disclose any PII to any other party without the prior written consent of the parent or eligible student:

1. Except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with law, regulation, and its contract with the District; or

2. Unless required by law or court order and the third-party contractor provides a notice of the disclosure to NYSED, the Board, or the institution that provided the information no later than the time the information is disclosed, unless providing notice of the disclosure is expressly prohibited by law or court order;

f) Maintain reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of PII in its custody;

g) Use encryption to protect PII in its custody while in motion or at rest; and

h) 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.

Where a third-party contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by law and contract apply to the subcontractor.

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

Cooperative Educational Services through a BOCES

The District may not be required to enter into a separate contract or data sharing and confidentiality agreement with a third-party contractor that will receive student data or teacher or principal data from the District under all circumstances.

For example, the District may not need its own contract or agreement where:

a) It has entered into a cooperative educational service agreement (CoSer) with a BOCES that includes use of a third-party contractor's product or service; and

b) That BOCES has entered into a contract or data sharing and confidentiality agreement with the third-party contractor, pursuant to Education Law Section 2-d and its implementing regulations, that is applicable to the District's use of the product or service under that CoSer.

To meet its obligations whenever student data or teacher or principal data from the District is received by a third-party contractor pursuant to a CoSer, the District will consult with the BOCES to, among other things:

a) Ensure there is a contract or data sharing and confidentiality agreement pursuant to Education Law Section 2-d and its implementing regulations in place that would specifically govern the District's use of a third-party contractor's product or service under a particular CoSer;

b) Determine procedures for including supplemental information about any applicable contracts or data sharing and confidentiality agreements that a BOCES has entered into with a third-party contractor in its Parents' Bill of Rights for Data Privacy and Security;

c) Ensure appropriate notification is provided to affected parents, eligible students, teachers, and/or principals about any breach or unauthorized release of PII that a third-party contractor has received from the District pursuant to a BOCES contract; and

d) Coordinate reporting to the Chief Privacy Officer to avoid duplication in the event the District receives information directly from a third-party contractor about a breach or unauthorized release of PII that the third-party contractor received from the District pursuant to a BOCES contract.

Click-Wrap Agreements

Periodically, District staff may wish to use software, applications, or other technologies in which the user must "click" a button or box to agree to certain online terms of service prior to using the software, application, or other technology. These are known as "click-wrap agreements" and are considered legally binding "contracts or other written agreements" under Education Law Section 2-d and its implementing regulations.

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

District staff are prohibited from using software, applications, or other technologies pursuant to a click-wrap agreement in which the third-party contractor receives student data or teacher or principal data from the District unless they have received prior approval from the District's Data Protection Officer or designee.

The District will develop and implement procedures requiring prior review and approval for staff use of any software, applications, or other technologies pursuant to click-wrap agreements.

Parents' Bill of Rights for Data Privacy and Security

The District will publish its Parents' Bill of Rights for Data Privacy and Security (Bill of Rights) on its website. Additionally, the District will include the Bill of Rights with every contract or other written agreement it enters into with a third-party contractor under which the third-party contractor will receive student data or teacher or principal data from the District.

The Bill of Rights will contain all required elements including supplemental information for each contract the District enters into with a third-party contractor where the third-party contractor receives student data or teacher or principal data from the District. The supplemental information must be developed by the District and include the following information:

a) The exclusive purposes for which the student data or teacher or principal data will be used by the third-party contractor, as defined in the contract;

b) How the third-party contractor will ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable laws and regulations (e.g., FERPA; Education Law Section 2-d);

c) The duration of the contract, including the contract's expiration date, and a description of what will happen to the student data or teacher or principal data upon expiration of the contract or other written agreement (e.g., whether, when, and in what format it will be returned to the District, and/or whether, when, and how the data will be destroyed);

d) If and how a parent, student, eligible student, teacher, or principal may challenge the accuracy of the student data or teacher or principal data that is collected;

e) Where the student data or teacher or principal data will be stored, described in a manner as to protect data security, and the security protections taken to ensure the data will be protected and data privacy and security risks mitigated; and

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

f) Address how the data will be protected using encryption while in motion and at rest.

The 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 District. The Bill of Rights and supplemental information may be redacted to the extent necessary to safeguard the privacy and/or security of the District's data and/or technology infrastructure.

Right of Parents and Eligible Students to Inspect and Review Students' Education Records

Consistent with the obligations of the District under FERPA, parents and eligible students have the right to inspect and review a student's education record by making a request directly to the District in a manner prescribed by the District.

The District will ensure that only authorized individuals are able to inspect and review student data. To that end, the District will take steps to verify the identity of parents or eligible students who submit requests to inspect and review an education record and verify the individual's authority to do so.

Requests by a parent or eligible student for access to a student's education records must be directed to the District and not to a third-party contractor. The District may require that requests to inspect and review education records be made in writing.

The District will notify parents annually of their right to request to inspect and review their child's education record including any student data stored or maintained by the District through its annual FERPA notice. A notice separate from the District's annual FERPA notice is not required.

The District will comply with a request for access to records within a reasonable period, but not more than 45 calendar days after receipt of a request.

The District may provide the records to a parent or eligible student electronically, if the parent consents. The District must transmit the PII in a way that complies with laws and regulations. Safeguards associated with industry standards and best practices, including but not limited to encryption and password protection, must be in place when education records requested by a parent or eligible student are electronically transmitted.

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

Complaints of Breach or Unauthorized Release of Student Data and/or Teacher or Principal Data

The District will inform parents, through its Parents' Bill of Rights for Data Privacy and Security, that they have the right to submit complaints about possible breaches of student data to the Chief Privacy Officer at NYSED. In addition, the District has established the following procedures for parents, eligible students, teachers, principals, and other District staff to file complaints with the District about breaches or unauthorized releases of student data and/or teacher or principal data:

a) All complaints must be submitted to the District's Data Protection Officer in writing.

b) Upon receipt of a complaint, the District will promptly acknowledge receipt of the complaint, commence an investigation, and take the necessary precautions to protect PII.

c) Following the investigation of a submitted complaint, the District will provide the individual who filed the complaint with its findings. This will be completed within a reasonable period of time, but no more than 60 calendar days from the receipt of the complaint by the District.

d) If the District requires additional time, or where the response may compromise security or impede a law enforcement investigation, the District will provide the individual who filed the complaint with a written explanation that includes the approximate date when the District anticipates that it will respond to the complaint.

These procedures will be disseminated to parents, eligible students, teachers, principals, and other District staff.

The 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.

Reporting a Breach or Unauthorized Release

The District will report every discovery or report of a breach or unauthorized release of student data or teacher or principal data within the District to the Chief Privacy Officer without unreasonable delay, but no more than ten calendar days after the discovery.

Each third-party contractor that receives student data or teacher or principal data pursuant to a contract or other written agreement entered into with the District will be required to promptly notify the District of any breach of security resulting in an unauthorized release of the data by the third-party contractor or its assignees in violation of applicable laws and regulations, the Parents' Bill of Rights for Student Data Privacy and Security, District policy, and/or binding contractual obligations relating to data privacy and security, in the most expedient way possible and without unreasonable delay, but no more than seven calendar days after the discovery of the breach.

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

In the event of notification from a third-party contractor, the District will in turn notify the Chief Privacy Officer of the breach or unauthorized release of student data or teacher or principal data no more than ten calendar days after it receives the third-party contractor's notification using a form or format prescribed by NYSED.

Investigation of Reports of Breach or Unauthorized Release by the Chief Privacy Officer

The Chief Privacy Officer is required to investigate reports of breaches or unauthorized releases of student data or teacher or principal data by third-party contractors. As part of an investigation, the Chief Privacy Officer may require that the parties submit documentation, provide testimony, and may visit, examine, and/or inspect the third-party contractor's facilities and records.

Upon the belief that a breach or unauthorized release constitutes criminal conduct, the Chief Privacy Officer is required to report the breach and unauthorized release to law enforcement in the most expedient way possible and without unreasonable delay.

Third-party contractors are required to cooperate with the District and law enforcement to protect the integrity of investigations into the breach or unauthorized release of PII.

Upon conclusion of an investigation, if the Chief Privacy Officer determines that a third-party contractor has through its actions or omissions caused student data or teacher or principal data to be breached or released to any person or entity not authorized by law to receive this data in violation of applicable laws and regulations, District policy, and/or any binding contractual obligations, the Chief Privacy Officer is required to notify the third-party contractor of the finding and give the third-party contractor no more than 30 days to submit a written response.

If after reviewing the third-party contractor's written response, the Chief Privacy Officer determines the incident to be a violation of Education Law Section 2-d, the Chief Privacy Officer will be authorized to:

a) Order the third-party contractor be precluded from accessing PII from the affected educational agency for a fixed period of up to five years;

b) Order that a third-party contractor or assignee who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data be precluded from accessing student data or teacher or principal data from any educational agency in the state for a fixed period of up to five years;

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

c) Order that a third-party contractor who knowingly or recklessly allowed for the breach or unauthorized release of student data or teacher or principal data will not be deemed a responsible bidder or offeror on any contract with an educational agency that involves the sharing of student data or teacher or principal data, as applicable for purposes of General Municipal Law Section 103 or State Finance Law Section 163(10)(c), as applicable, for a fixed period of up to five years; and/or

d) Require the third-party contractor to provide additional training governing confidentiality of student data and/or teacher or principal data to all its officers and employees with reasonable access to this data and certify that the training has been performed at the contractor's expense. This additional training is required to be performed immediately and include a review of laws, rules, and regulations, including Education Law Section 2-d and its implementing regulations.

If the Chief Privacy Officer determines that the breach or unauthorized release of student data or teacher or principal data on the part of the third-party contractor or assignee was inadvertent and done without intent, knowledge, recklessness, or gross negligence, the Chief Privacy Officer may make a recommendation to the Commissioner that no penalty be issued to the third-party contractor.

The Commissioner would then make a final determination as to whether the breach or unauthorized release was inadvertent and done without intent, knowledge, recklessness or gross negligence and whether or not a penalty should be issued.

Notification of a Breach or Unauthorized Release

The District will notify affected parents, eligible students, teachers, and/or principals in the most expedient way possible and without unreasonable delay, but no more than 60 calendar days after the discovery of a breach or unauthorized release of PII by the District or the receipt of a notification of a breach or unauthorized release of PII from a third-party contractor unless that notification would interfere with an ongoing investigation by law enforcement or cause further disclosure of PII by disclosing an unfixed security vulnerability. Where notification is delayed under these circumstances, the District will notify parents, eligible students, teachers, and/or principals within seven calendar days after the security vulnerability has been remedied or the risk of interference with the law enforcement investigation ends.

Notifications will be clear, concise, use language that is plain and easy to understand, and to the extent available, include:

a) A brief description of the breach or unauthorized release, the dates of the incident and the date of discovery, if known;

(Continued)

SUBJECT: PRIVACY AND SECURITY FOR STUDENT DATA AND TEACHER AND PRINCIPAL DATA (Cont'd.)

b) A description of the types of PII affected;

c) An estimate of the number of records affected;

d) A brief description of the District's investigation or plan to investigate; and

e) Contact information for representatives who can assist parents or eligible students that have additional questions.

Notification will be directly provided to the affected parent, eligible student, teacher, or principal by first-class mail to their last known address, by email, or by telephone.

Where a breach or unauthorized release is attributed to a third-party contractor, the third-party contractor is required to pay for or promptly reimburse the District for the full cost of this notification.

Annual Data Privacy and Security Training

The District will annually provide data privacy and security awareness training to its officers and staff with access to PII. This training will include, but not be limited to, training on the applicable laws and regulations that protect PII and how staff can comply with these laws and regulations. The District may deliver this training using online training tools. Additionally, this training may be included as part of the training that the District already offers to its workforce.

Notification of Policy

The District will publish this policy on its website and provide notice of the policy to all its officers and staff.

Education Law § 2-d
8 NYCRR Part 121

Adoption Date

SUBJECT: SCHOOL SAFETY PLANS

The District considers the safety of its students and staff to be of the utmost importance and is keenly aware of the evolving nature of threats to schools. As such, it will address those threats accordingly through appropriate emergency response planning. The District-wide school safety plan and the building-level emergency response plan(s) will be designed to prevent or minimize the effects of violent incidents and emergencies and to facilitate the coordination of schools and the District with local and county resources in the event of these incidents or emergencies. These plans will be reviewed and updated by the appropriate team on at least an annual basis and adopted by the Board by September 1 of each school year.

The Board will make the District-wide school safety plan available for public comment at least 30 days prior to its adoption. The District-wide school safety plan may only be adopted by the Board after at least one public hearing that provides for the participation of school personnel, parents, students, and any other interested parties. The District-wide school safety plan and any amendments must be submitted to the Commissioner, in a manner prescribed by the Commissioner, within 30 days of adoption, but no later than October 1 of each school year.

Building-level emergency response plan(s) and any amendments must be submitted to the appropriate local law enforcement agency and the state police within 30 days of adoption, but no later than October 1 of each school year. Building-level emergency response plan(s) will be kept confidential and are not subject to disclosure under the Freedom of Information Law (FOIL) or any other provision of law.

District-Wide School Safety Plan

District-wide school safety plan means a comprehensive, multi-hazard school safety plan that covers all school buildings of the District, addresses crisis intervention, emergency response and management at the District level, and has the contents as prescribed in Education Law and Commissioner's regulations.

The District-wide school safety plan will be developed by the District-wide school safety team appointed by the Board. The District-wide school safety team will include, but not be limited to, representatives of the Board, teacher, administrator, and parent organizations, school safety personnel, and other school personnel including bus drivers and monitors. *At the discretion of the Board, a student may be allowed to participate on the District-wide school safety team.

The District-wide school safety plan will include, but not be limited to:

a) Policies and procedures for responding to implied or direct threats of violence by students, teachers, other school personnel including bus drivers and monitors, and visitors to the school, including threats by students against themselves, which includes suicide;

** Allowing a student member to participate on the safety team is now optional, not required. Please customize accordingly. A student may participate provided that no confidential information is shared with that student.*

(Continued)

SUBJECT: SCHOOL SAFETY PLANS (Cont'd.)

b) Policies and procedures for responding to acts of violence by students, teachers, other school personnel including bus drivers and monitors, and visitors to the school, including consideration of zero-tolerance policies for school violence;

c) Appropriate prevention and intervention strategies, such as:

1. Collaborative arrangements with state and local law enforcement officials, designed to ensure that school safety officers and other security personnel are adequately trained, including being trained to de-escalate potentially violent situations, and are effectively and fairly recruited;

2. Nonviolent conflict resolution training programs;

3. Peer mediation programs and youth courts; and

4. Extended day and other school safety programs;

d) Policies and procedures for contacting appropriate law enforcement officials in the event of a violent incident;

e) A description of the arrangements for obtaining assistance during emergencies from emergency services organizations and local governmental agencies;

f) Procedures for obtaining advice and assistance from local government officials, including the county or city officials responsible for implementation of Executive Law Article 2-B, State and Local Natural and Man-Made Disaster Preparedness;

g) The identification of District resources which may be available for use during an emergency;

h) A description of procedures to coordinate the use of District resources and manpower during emergencies, including identification of the officials authorized to make decisions and of the staff members assigned to provide assistance during emergencies;

i) Policies and procedures for contacting parents, guardians, or persons in parental relation to District students in the event of a violent incident or an early dismissal;

j) Policies and procedures for contacting parents, guardians, or persons in parental relation to an individual District student in the event of an implied or direct threat of violence by the student against themselves, which includes suicide;

k) Policies and procedures relating to school building security, including, where appropriate: the use of school safety officers, school security officers, and/or school resource officers; and security devices or procedures;

(Continued)

SUBJECT: SCHOOL SAFETY PLANS (Cont'd.)

l) Policies and procedures for the dissemination of informative materials regarding the early detection of potentially violent behaviors, including, but not limited to, the identification of family, community, and environmental factors to teachers, administrators, school personnel including bus drivers and monitors, parents and other persons in parental relation to students of the District or Board, students, and other persons deemed appropriate to receive the information;

m) Policies and procedures for annual multi-hazard school safety training for staff and students, provided that the District must certify to the Commissioner that all staff have undergone annual training by September 15 on the building-level emergency response plan which must include components on violence prevention and mental health, provided further that new employees hired after the start of the school year will receive training within 30 days of hire or as part of the District's existing new hire training program, whichever is sooner;

n) Procedures for the review and conduct of drills and other exercises to test components of the emergency response plan, including the use of tabletop exercises, in coordination with local and county emergency responders and preparedness officials;

o) The identification of appropriate responses to emergencies, including protocols for responding to bomb threats, hostage-takings, intrusions, and kidnappings;

p) Strategies for improving communication among students and between students and staff and reporting of potentially violent incidents, such as the establishment of youth-run programs, peer mediation, conflict resolution, creating a forum or designating a mentor for students concerned with bullying or violence, and establishing anonymous reporting mechanisms for school violence;

q) A description of the duties of hall monitors and any other school safety personnel, the training required of all personnel acting in a school security capacity, and the hiring and screening process for all personnel acting in a school security capacity;

r) A system for informing all educational agencies within the District of a disaster;

s) The designation of the Superintendent or designee, as the District Chief Emergency Officer whose duties will include, but not be limited to:

1. Coordinating the communication between school staff, law enforcement, and other first responders;

2. Leading the efforts of the District-wide school safety team in the completion and yearly update of the District-wide school safety plan and the coordination of the District-wide school safety plan with the building-level emergency response plan(s);

(Continued)

SUBJECT: SCHOOL SAFETY PLANS (Cont'd.)

3. Ensuring staff understanding of the District-wide school safety plan;

4. Ensuring the completion and yearly update of building-level emergency response plans for each school building;

5. Assisting in the selection of security related technology and development of procedures for the use of the technology;

6. Coordinating appropriate safety, security, and emergency training for District and school staff, including required training in the emergency response plan;

7. Ensuring the conduct of required evacuation and lock-down drills in all District buildings as required by law; and

8. Ensuring the completion and yearly update of building-level emergency response plan(s) by the dates designated by the Commissioner; and

t) Protocols for responding to a declared state disaster emergency involving a communicable disease that are substantially consistent with the provisions in Labor Law Section 27-c.

Building-Level Emergency Response Plan

Building-level emergency response plan means a building-specific school emergency response plan that addresses crisis intervention, emergency response and management at the building level and has the contents as prescribed in Education Law and Commissioner's regulations. As part of this plan, the District will define the chain of command in a manner consistent with the National Incident Management System (NIMS)/Incident Command System (ICS).

Building-level emergency response plan(s) will be developed by the building-level emergency response team. The building-level emergency response team is a building-specific team appointed by the building principal, in accordance with regulations or guidelines prescribed by the Board. The building-level emergency response team will include, but not be limited to, representatives of teacher, administrator, and parent organizations, school safety personnel and other school personnel including bus drivers and monitors, community members, local law enforcement officials, local ambulance, fire officials, or other emergency response agencies, and any other representatives the Board deems appropriate.

Classroom door vision panels will not be covered except as outlined in the building-level emergency response plan.

Education Law § 2801-a
Labor Law § 27-c
8 NYCRR § 155.17

Adoption Date

SUBJECT: EMPLOYMENT OF RELATIVES OF BOARD MEMBERS

The District will not employ any teacher who is related by blood or marriage to any Board member unless two-thirds of the Board members consent at a Board meeting. The vote will be recorded in the Board's meeting minutes.

Education Law § 3016
General Municipal Law §§ 800-809

Adoption Date

SUBJECT: STUDENT RECORDS: ACCESS AND CHALLENGE

The District will comply with the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA). Under its provisions, parents or guardians and non-custodial parent(s) whose rights are not limited by court order or formal agreement, of a student under 18, or a student who is 18 years of age or older, or who is attending an institution of post-secondary education, have a right to inspect and review any and all education records maintained by the District.

Education Records

The term "education records" is defined as all records, files, documents, and other materials containing information directly related to a student; and maintained by the education agency or institution, or by a person acting for that agency or institution. This includes all records regardless of medium, including, but not limited to, handwriting, videotape or audiotape, electronic or computer files, film, print, microfilm, and microfiche.

In addition, for students who attend a public school district, all records pertaining to services provided under the Individuals with Disabilities Education Act (IDEA) are considered "education records" under FERPA and they are subject to the confidentiality provisions of both Acts.

However, personal notes made by teachers or other staff are not considered education records if they are:

a) Kept in the sole possession of the maker;

b) Not accessible or revealed to any other person except a temporary substitute; and

c) Used only as a memory aid.

Additionally, FERPA does not prohibit a school official from disclosing information about a student if the information is obtained through the school official's personal knowledge or observation and not from the student's education records.

Records created and maintained by a law enforcement unit for law enforcement purposes are also excluded.

Access to Student Records

Administrative regulations and procedures will be developed to comply with the provisions of federal law relating to the availability of student records. The purpose of these regulations and procedures is to make available to the parents or guardians of students and non-custodial parent(s) whose rights are not limited by court order or formal agreement, or students who are 18 years of age or older, or who are attending an institution of post-secondary education, student records, and files on students, and to ensure the confidentiality of these records with respect to third parties.

(Continued)

SUBJECT: STUDENT RECORDS: ACCESS AND CHALLENGE (Cont'd.)

Under FERPA, unless otherwise exempted in accordance with law and regulation, the District may release personally identifiable information (PII) contained in student education records only if it has received a "signed and dated written consent" from a parent or eligible student. Signed and dated written consent may include a record and signature in electronic form provided that the signature:

a) Identifies and authenticates a particular person as the source of the electronic consent; and

b) Indicates the person's approval of the information contained in the electronic consent.

Exceptions

Without the consent of a parent or eligible student, the District may release a student's information or records when it is:

a) Directory Information and Limited Directory Information

"Directory information" is information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. "Limited Directory Information Disclosure" means that the District may limit disclosure of its designated directory information to specific parties, for specific purposes, or both. The intent is to allow schools the option to implement policies that allow for the disclosure of student information for uses such as yearbooks, honor roll lists, graduation programs, and playbills, but restrict disclosure for more potentially dangerous purposes. The District will limit disclosure of its designated directory information as otherwise specified in its public notice to parents of students in attendance and eligible students in attendance.

b) To School Officials who have a Legitimate Educational Interest

To other school officials, including teachers, within the educational agency or institution whom the school has determined to have legitimate educational interests. An educational interest includes the behavior of a student and disciplinary action taken against the student for conduct that posed a significant risk to the safety or well-being of the student, other students, or other members of the school community. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibility.

c) To Another Educational Institution

The District may disclose any and all educational records, including disciplinary records and records that were created as a result of a student receiving special education services under Part B of IDEA, to another school or post-secondary institution at which the student seeks or intends to enroll, or after the student has enrolled or transferred, so long as the disclosure

(Continued)

is for purposes related to the student's enrollment or transfer. Parental consent is not required for transferring education records if the school's annual FERPA notification indicates that these disclosures may be made. In the absence of information about disclosures in the annual FERPA notification, school officials must make a reasonable attempt to notify the parent about the disclosure, unless the parent initiated the disclosure. Additionally, upon request, the District will provide a copy of the information disclosed and an opportunity for a hearing.

d) For Health and Safety Emergency Reasons

The District must balance the need to protect students' PII with the need to address issues of school safety and emergency preparedness. Under FERPA, if an educational agency or institution determines that there is an articulable and significant threat to the health or safety of a student or other individuals, it may disclose information from education records, without consent, to any person whose knowledge of the information is necessary to protect the health and safety of the student or other individuals during the period of the health or safety emergency. The District may release information from records to appropriate parties including, but not limited to, parents, law enforcement officials, and medical personnel. The District's determination that there is an articulable and significant threat to the health or safety of a student or other individuals will be based upon a totality of the circumstances, including the information available, at the time the determination is made. The District must record the articulable and significant threat that formed the basis for the disclosure and maintain this record for as long as the student's education records are maintained.

e) To Juvenile Justice Systems

Information may be disclosed to state and local officials or authorities to whom information is specifically allowed to be reported or disclosed by a state statute that concerns the juvenile justice system and the system's ability to effectively serve, prior to adjudication, the student whose records were released. In these cases, the official or authority must certify in writing that the information will not be disclosed to any other party except as provided under law without prior written consent.

f) To Foster Care Agencies

The District may release records to an agency caseworker or other representative of a state or local child welfare agency, who has the right to access a student's case plan, when the agency or organization is legally responsible, for the care and protection of the student. This does not give a child welfare agency the right to look into any non-foster care student's records, without parental consent, when there has been a mere allegation of abuse or maltreatment, absent an order or subpoena.

(Continued)

SUBJECT: STUDENT RECORDS: ACCESS AND CHALLENGE (Cont'd.)

g) Pursuant to a Subpoena or Court Order

When the District receives a subpoena or court order for the release of records, it will make a reasonable effort to notify the parent or guardian or eligible student of the order or subpoena in advance of compliance. This allows the parent or guardian or eligible student to seek protective action against the subpoena or order before the release of the records.

The District may disclose a student's records without first notifying parents or guardians or eligible students if the disclosure is:

1. Based on a subpoena in which the court orders, for good cause shown, not to reveal to any person the existence or contents of the subpoena or any information furnished pursuant to the subpoena;

2. In accordance with a judicial order in cases where the parents are a party to a court proceeding involving child abuse or maltreatment or dependency matters, and the order is issued in the context of that proceeding; or

3. Made to a court (with or without an order or subpoena) when the District is involved in a legal action against a parent or student and the records are relevant to the matter.

h) For Financial Aid Purposes

Pertinent information may be released in connection with the determination of eligibility, amount, conditions, and enforcement of terms of a student's financial aid.

i) To Accrediting Organizations

Disclosure of a student's records may be made to an organization in which that student seeks accreditation, in order to carry out their accrediting function.

j) To Parents of a Dependent Student

Even when a student turns 18 years of age or older the District may disclose education records to that student's parents, without the student's consent, if the student is claimed as a dependent for federal income tax purposes by either parent.

k) For Audit/Evaluation Purposes

The audit or evaluation exception allows for the disclosure of PII from education records without consent to authorized representatives of the Comptroller General of the U.S., the Attorney General, the Secretary of Education, federal, state, or local educational authorities.

(Continued)

SUBJECT: STUDENT RECORDS: ACCESS AND CHALLENGE (Cont'd.)

Under this exception, PII from education records must be used to audit or evaluate a federal or state supported education program, or to enforce or comply with federal legal requirements that relate to those education programs.

The District may occasionally disclose PII from education records without consent to authorized representatives of the entities listed above. The District may also designate its own authorized representative who may access PII without consent in connection with an audit or evaluation of an education program within the District. As an example, the District might designate a university as its authorized representative in order to disclose, without consent, PII from education records on its former students to the university. The university could then disclose, without consent, transcript data on those former students attending the university to allow the District to evaluate how effectively the District prepared its students for success in post-secondary education.

l) For Conducting Studies

This exception allows for the disclosure of PII from education records without consent to organizations conducting studies for, or on behalf of, schools, school districts, or post-secondary institutions. Studies can be for the purpose of developing, validating, or administering predictive tests, administering student aid programs, or improving instruction.

The District may disclose PII from education records without consent to these organizations conducting studies for the District, in accordance with its obligations under FERPA.

In addition, other entities outside of the District may occasionally disclose PII from education records that the District has previously shared with that entity, to organizations conducting studies on behalf of the District. For example, a State Education Agency (SEA) may disclose PII from education records provided by the District without consent to an organization for the purpose of conducting a study that compares program outcomes across school districts to further assess the effectiveness of these programs with the goal of providing the best instruction.

Required Agreements for the Studies or Audit/Evaluation Exceptions (see items k and l)

To the extent required by law, the District will enter into a written agreement with organizations conducting studies for the District, or, with its designated authorized representatives in connection with audits or evaluations of education programs within the District. In the event that the District discloses PII from education records to its own designated authorized representative in connection with an audit or evaluation of an educational program within the District, it will use reasonable methods to ensure to the greatest extent practicable that its designated authorized representative complies with FERPA and its regulations.

(Continued)

SUBJECT: STUDENT RECORDS: ACCESS AND CHALLENGE (Cont'd.)

Challenge to Student Records

Parents or guardians of a student under the age of 18, or a student who is 18 years of age or older or who is attending an institution of post-secondary education, will have an opportunity for a hearing to challenge the content of the school records and to ensure that the records are not inaccurate, misleading, or otherwise in violation of the privacy of students, and to provide an opportunity for the correction or deletion of any inaccurate, misleading, or otherwise inappropriate data.

Release of Information to the Non-Custodial Parent

The District may presume that the non-custodial parent has the authority to request information concerning his or her child and release this information upon request. If the custodial parent wishes to limit the non-custodial parent's access to the records, it is his or her responsibility to obtain and present to the school a legally binding instrument that prevents the release of information related to the child.

Family Educational Rights and Privacy Act of 1974, 20 USC § 1232g
34 CFR Part 99
Education Law § 2-d

NOTE: Refer also to Policies #5676 -- Privacy and Security for Student Data and Teacher and Principal Data
#7241 -- Student Directory Information
#7242 -- Military Recruiters and Institutions of Higher Education
#7643 -- Transfer Students with Disabilities

Adoption Date

SUBJECT: PATRIOTISM, CITIZENSHIP, AND HUMAN RIGHTS EDUCATION

In order to promote a spirit of patriotic and civil service and obligation, as well as to foster in students of the District moral and intellectual qualities which are essential in preparing them to meet the obligations of citizenship, the Board requires students attending District schools, over the age of eight years, to attend instructional courses in patriotism, citizenship, civic education and values, our shared history of diversity, the role of religious tolerance in this country, and human rights issues, with particular attention to the study of the inhumanity of genocide, slavery (including the Freedom Trail and Underground Railroad), the Holocaust, and the mass starvation in Ireland from 1845 to 1850.

The Board also directs that all students attending District schools in grades 8 through 12 receive instruction in the history, meaning, significance and effect of the United States Constitution, the New York State Constitution, and the Declaration of Independence.

The curricula for these courses must include the subjects specified by the Board of Regents and be for the period of instruction, as mandated by the Regents, which is necessary in these subjects in each of the appropriate grades.

One week during each school year a uniform course of exercises will be provided to teach students, in an age appropriate manner, the purpose, meaning, and importance of the Bill of Rights Articles in the United States and New York State Constitutions. These exercises will be in addition to the above required courses.

In addition, since the District receives Federal Funds for a fiscal year, it will hold an educational program on the United States Constitution on September 17th of each year for the students in the District to commemorate the September 17, 1787 signing of the Constitution, known as Constitution Day and Citizenship Day. However, when September 17 falls on a Saturday, Sunday, or holiday, this day will be held during the preceding or following week.

The Board directs that the above named subjects, as mandated by law, be addressed in the instructional curricula provided by the District.

36 USC § 106
Education Law § 801
8 NYCRR § 100.2(c)

NOTE: Refer also to Policies #3430 -- Diversity, Equity, and Inclusion in the District
#8242 -- Civility, Citizenship, and Character Education/Interpersonal Violence Prevention Education

Adoption Date