8000

[ ] Required
[X] Local
[ ] Notice

SUPPORT SERVICES GOALS

Support services, which include safety and maintenance programs, transportation, insurance management and office services, are essential to the successful functioning of the school district. Education is the district's central function, and all support services shall be provided, guided, and evaluated by this function.

In order to provide services that are truly supportive of the educational program, the Board of Trustees establishes these goals:

1. providing a physical environment for teaching and learning that is safe and pleasant for students, staff, and the public;
2. providing safe transportation for students who use these services; and
3. providing timely, accurate, and efficient support services that meet district needs and promote district goals.

Adoption date: 6/11/13

8110

[ ] Required
[X] Local
[ ] Notice

SCHOOL BUILDING SAFETY

The Board of Trustees recognizes that a safe, secure and healthy school environment is necessary to promote effective learning. The Board is committed to ensuring that all school buildings are properly maintained and preserved to provide a suitable educational setting.

Consistent with the requirements of state law and regulations, the Board will:

1. Appoint a Health and Safety Committee composed of representation from district administration, school staff, bargaining units and parents that shall participate in monitoring the condition of occupied school buildings to assure that they are safe and maintained in a state of good repair. (The members of the District's Shared Decision-Making Committee (SDMC) will also serve as the District's Health and Safety Committee and will complete all tasks related to this requirement.)
2. Review and approve all annual building inspections and building condition surveys, and when required by the State or the Commissioner of Education, visual inspections.
3. Take immediate action to remedy serious conditions in school buildings affecting health and safety and report such conditions to the Commissioner of Education.

The Superintendent of Schools shall be responsible for the development of procedures for investigating and resolving complaints related to the health and safety issues in the district's buildings consistent with requirements of state law and regulations.

Cross-ref: 7100, Facilities Planning
7365, Construction Safety
8112, Health and Safety Committee
8220, Buildings and Grounds Maintenance and Inspection

Ref: Education Law §§ 409-d (Comprehensive Public School Building Safety Program); 409-e (Uniform Code of Public School Buildings Inspection, Safety Rating and Monitoring)
8 NYCRR Part 155 (Educational Facilities)
9 NYCRR Parts 600-1250 (Uniform Fire Prevention and Building Code)

Adoption date: 6/11/13
Amended date: 12/17/15
Amended date: 10/21/21

8112

[ ] Required
[X] Local
[ ] Notice

HEALTH AND SAFETY COMMITTEE

The Board of Trustees recognizes the importance of the participation of district staff and parents in promoting a safe, secure and healthy school environment. In accordance with Commissioner's regulations, the Board will appoint a Health and Safety Committee composed of representation from district officials, staff, bargaining units and parents. (The members of the District's Shared Decision-Making Committee (SDMC) will also serve as the District Health and Safety Committee and will complete all tasks related to this requirement.)

The committee will participate in monitoring the condition of occupied school buildings to assure that they are safe and maintained in a state of good repair. The Superintendent of Schools will ensure that the committee is appropriately involved in all of the activities required by the Commissioner's regulations. Specifically, the committee will:

1. Participate in the investigation and disposition of health and safety complaints.
2. Ensure that at least one member of the committee participates in the annual visual inspection.
3. Consult with district officials in completing safety ratings of all occupied school buildings.
4. Monitor safety during school construction projects including periodic meetings to review issues and address complaints related to health and safety resulting from the project.
5. Upon completion of a construction project, conduct a walk-through inspection to ensure the area is ready to be reopened for use.

Expanded Health and Safety Committee

During construction projects, the Health and Safety Committee will be expanded to include the architect, construction manager and contractor. This expanded committee will:

1. Participate in the investigation and disposition of health and safety complaints regarding the construction or maintenance project.
2. Meet periodically to review issues and address complaints regarding health and safety arising from construction.
3. Monitor safety during construction projects.
4. After the work is completed, conduct a walk-through inspection to confirm that the area is ready to be reopened for use.
5. Ensure that at least one member of the committee participates in any visual inspection required by the State or Commissioner of Education.

Ref.: 8 NYCRR Part 155 (Educational Facilities)
Adoption date: 12/17/15
Amended date: 10/21/21

8115
[ ] Required
[ ] Local
[X] Notice

PESTICIDES AND PEST MANAGEMENT

It is the goal of the Board of Trustees to maintain the integrity of school buildings and grounds, protect the health and safety of students and staff and maintain a productive learning environment.

The Board recognizes that pests can pose a significant risk to health and property and there may be significant risks inherent in using chemical pesticides in the school environment. Provisions will be made for a least toxic approach to integrated pest management (IPM) for the school building and grounds in accordance with the Commissioner's regulations. Integrated pest management is a systematic approach to managing pests focusing on long term prevention or suppression with minimal impact on human health, the environment and non-targeted organisms.

Notification of Pesticide Application

All district staff and parents/guardians will be notified of pesticide applications performed at the school facility. A notice will be sent at the beginning of the school year which will include:

1. Notification of periodic pesticide applications throughout school year.
2. The availability of 48-hour prior written notification of pesticide applications to parents and staff who request such notice.
3. Instructions on how to register with the school to receive this prior written notification.
4. The name and number of the school representative who can provide further information.

The Superintendent of Schools shall ensure the dissemination of this policy and conduct any training necessary to ensure that all staff are fully informed about pesticides and pest management.

Cross-ref: 8110, School Building Safety
8220, Building and Grounds Maintenance and Inspection

Ref: Environmental Conservation Law, Art.33 (Pesticides)
Education Law §409-h (Requirements for Notification of Pesticide Applications)
6 NYCRR Part 325 (Application of Pesticides)
8 NYCRR §155.4 (Uniform Code of Public School Building Inspections, Safety Rating and Monitoring)
Desmond Americana v. Jorling, 153 AD2d 4 (3rd Dept. 1989)
IPM Workbook for New York State Schools, Cornell Cooperative Extension Community IPM Program with support from New York State Dept. of Environmental Conservation, August 1998

Adoption date: 6/11/13

8123

( ) Required
(X) Local
(X) Notice

HYGIENE PRECAUTIONS AND PROCEDURES

The Board of Trustees, in order to promote and ensure the health and safety of all students and staff, adopts the following policy on hygiene and sanitary procedures for dealing with exposure to and contact with blood and other body fluids.

To prevent and/or minimize the transmission of contagious or communicable diseases or infections within the school community, all employees of the school district shall utilize appropriate precautions when providing first aid or otherwise dealing with situations that involve exposure to blood and other body fluids. Such precautionary measures will be followed uniformly in all instances and shall be applicable throughout the school district.

The Superintendent of Schools is responsible for developing appropriate procedures to implement this policy and for informing all staff of such procedures and ensuring compliance with them. The failure to utilize such procedures may form the basis for disciplinary action.

Cross-ref: 5420, Student Health Services

Ref: State Sanitary Code, Chapter 1, Part 14

Adoption date: 3/14/19

8130

( ) Required
(X) Local
(X) Notice

SCHOOL SAFETY PLANS AND TEAMS

Emergencies and violent incidents in schools are critical issues that must be addressed in an expeditious and effective manner. The Board of Trustees recognizes its responsibility to adopt and keep current a comprehensive district wide school safety plan and building-level emergency response plan(s) which address violence prevention, crisis intervention, emergency response and management.

Taken together, the district-wide and building level plans will provide a comprehensive approach to addressing school safety and violence prevention, and provide the structure where all individuals can fully understand their roles and responsibilities for promoting the safety of the entire school community. The plans will be designed to prevent or minimize the effects of serious violent incidents and emergencies, declared state disaster emergencies involving a communicable disease or local public health emergency declaration and other emergencies and to facilitate the district's coordination with local and county resources. The plans will also address risk reduction/prevention, response and recovery with respect to a variety of types of emergencies and violent incidents in district schools, and will address school closures and continuity of operations

In accordance with state law and regulation, the district will have the following safety teams and plans to deal with violence prevention, crisis intervention and emergency response and management:

Comprehensive District-Wide School Safety Team and Plan

The Board will annually appoint a district-wide school safety team that includes, but is not be limited to, a representative from the following constituencies: the Board, teachers, administrators, and parent organizations, school safety personnel and other school personnel. (e.g. Transportation Coordinator) This team will be responsible for the development and annual review of the comprehensive district-wide school safety plan. The plan will cover all district school buildings and will address violence prevention (taking into consideration a range of programs and approaches that are designed to create a positive school climate and culture), crisis intervention, emergency response and management including communication protocols, at the district level. It will include all those elements required by law and regulation, including protocols for responding to declared state disaster emergencies involving a communicable disease that are substantially consistent with the provisions of Labor Law §27-c.

The Superintendent/Principal or his/her designee will be the district's chief emergency officer, and shall coordinate communication between school staff and law enforcement and first responders. The chief emergency officer will ensure that all staff understand the district-wide school safety plan and receive training on the building-level emergency response plan, violence prevention and mental health, and will also ensure that district-wide and building-level plans are completed, reviewed annually, and updated as needed by the designated dates. The chief emergency officer will ensure that the district-wide plan is coordinated with the building-level plans, and will ensure that required evacuation and lock-down drills are conducted.

Building-Level Emergency Response Plans and Teams

The Superintendent/Principal or his/her designee is responsible for annually appointing a building-level emergency response team that includes representation from teachers, administrators, parent organizations, school safety personnel (e.g. Transportation Coordinator), other school personnel, law enforcement officials, fire officials and other emergency response agencies. The emergency response team is responsible for the development and review of a building-level emergency response plan for each district building. The plan(s) shall address response to emergency situations, such as those requiring evacuation, sheltering and lock-down at the building level and will include all components required by law and regulation, including measures necessary to comply with Labor Law §27-c to respond to public health emergencies involving a communicable disease. These confidential plans will include evacuation routes, shelter sites, medical needs, transportation and emergency notification of parents and guardians.

Building-level emergency response plans will include protocols in response to carbon monoxide alarms or detection. Alarm or detection of carbon monoxide will result in the appropriate actions as described by the emergency response plan.

Building-level emergency response plans must designate:

- an emergency response team for incidents that includes appropriate school personnel, law enforcement officials, fire officials, and representatives from local, regional and/or state emergency response agencies to assist the school community in responding to a violent incident or emergency; and
- a post-incident response team that includes appropriate school personnel, medical personnel, mental health counselors and other related personnel to assist the community in coping with the aftermath of a serious violent incident or emergency.

During emergencies, staff are authorized to temporarily cover classroom door vision panels when it is likely to protect staff and students. For example, covering vision panels may prevent an intruder from determining if a classroom is occupied, thereby discouraging attempts to gain access. During emergencies, staff are also authorized to temporarily block doors to slow the access of intruders. Building-level emergency response plans must address the temporary covering of door vision panels and the temporary blocking of doors during emergencies.

The Superintendent/Principal or his/her designee is be responsible for conducting at least one test every school year of the emergency response procedures under this plan including procedures for sheltering and early dismissal.

To maintain security and in accordance with law, the building-level emergency response plan(s) shall be confidential and shall not be subject to disclosure under the Freedom of Information Law or any other law.

Threat Assessment Teams

The Superintendent/Principal or his/her designee, will annually designate a threat assessment team to provide ongoing support and information in order to identify, and assess individuals who may be potential threats to safety, with the intent of minimizing acts of violence in the school community. The threat assessment team will be composed of, but not limited to, the following personnel from both within the school and the larger community, as appropriate: building administrators, school nurse, school counselors, law enforcement and facilities/maintenance personnel. The team will meet yearly or as needed. The team will be mindful of the need for discretion and observance of confidentiality requirements.

Students will be encouraged to bring their concerns to any district employee. If a district employee becomes aware of a threat to the school community, they must inform the Superintendent/Principal or his/her designee and he/she will convene the threat assessment team. The Superintendent/Principal or his/her designee may request the participation of the following additional individuals who may have specific knowledge of the potential perpetrator: supervisors, teachers, students and parents. The Superintendent/Principal or his/her designee is responsible for keeping the Board of Trustees informed about the activities of the threat assessment team. Threat assessment team members shall receive appropriate training.

Annual Review and Reporting

All plans will be annually reviewed and updated, if necessary, by the appropriate team by July 15th. In conducting the review, the teams will consider any changes in organization, local conditions and other factors including an evaluation of the results of the annual test of the emergency response procedures which may necessitate updating of plans. If the plan requires no changes, then it will remain in effect. If the district-wide plan requires change, then the updated plan will be submitted to the Board of Trustees in time to allow 30-days of public comment and to hold a public hearing which provides for the participation of school personnel, students and other interested parties prior to Board adoption. All plans must be adopted by the Board of Trustees in September.

The Superintendent/Principal or his/her designee is responsible for submitting the district-level school safety plan and any amendments to the plan to the Commissioner within 30 days after its adoption, no later than October 1st of each year. The district-wide plan will be posted on the district's website. The Superintendent/Principal or his/her designee is responsible for submitting the building-level emergency response plan for his or her building, and any amendments to the plan, to the appropriate local law enforcement agency and the state police within 30 days after its adoption, but no later than October 15 of each year until the 2020-2021 school year when it must be submitted by October 1st.

Cross-ref: 0115, Bullying and Harassment Prevention and Intervention
5300, Code of Conduct
9700, Staff Development

Ref: Education Law §2801-a (school safety plans)
Executive Law §2B (state and local natural and manmade disaster preparedness)
8 NYCRR Part 155 (Educational Facilities)
School Safety Plans Guidance, New York State Education Department, June 2010

Adoption date: 6/11/13
Amendment date: 1/17/17
Amendment date: 7/9/2020
Amendment date: 8/17/21

8130.1

( ) Required
( ) Local
(X) Notice

EXTREME RISK PROTECTION ORDERS (THE "RED FLAG LAW")

Extreme risk protection orders are court orders that restrict the ability of a person, who is judged likely to engage in conduct that would result in serious physical harm to him/herself or others, to purchase or possess firearms, rifles or shotguns, or attempt to do so.

Under state law, the Superintendent/ Principal is permitted to petition the state Supreme Court for extreme risk protection orders for students currently enrolled in their building, or students who were enrolled in their building in the six months immediately before filing the petition (referred to in this policy as "currently-enrolled" and "recently-enrolled" students, respectively).

When district staff members have reason to believe, either personally or through information received by others, that a currently-enrolled or recently-enrolled student is likely to engage in conduct that would result in serious physical harm to him/herself or others, they are encouraged to report their concerns to the Superintendent/Principal or his/her designee. This is in keeping with employees' general responsibility for student safety, as well as their own interests for maintaining a safe working and learning environment.

Any other person, including but not limited to students, parents, and community members, may also bring their concerns to the Superintendent/Principal or his/her designee that a currently-enrolled or recently-enrolled student is likely to engage in conduct that would result in serious physical harm to him/herself or others.

If the Superintendent/Principal or his/her designee (Lead Teacher) is absent from the building, the Board of Trustees President will be the main point of contact to report concerns.

When a Superintendent/Principal receives concerns from persons under this policy, or has his/her own concerns about a student, he/she must immediately notify the Board of Trustees President. The Superintendent/Principal will contact the school attorney, and both will assist the Superintendent/Principal in determining the appropriateness of petitioning the court for an extreme risk protection order.

When determining whether it is appropriate to petition the court for an extreme risk protection order, the district will consider, among other things, the following factors as they relate to the student:

1. Threats or acts of violence or physical force made against him/herself or another person;
2. Violating or allegedly violating orders of protection (i.e., restraining orders);
3. Pending criminal convictions or charges involving weapons;
4. Recklessly using, displaying, or brandishing a firearm, rifle or shotgun;
5. Violating previous extreme risk protection orders;
6. Evidence of recent or current drug or alcohol abuse; and
7. Evidence that the student has recently acquired a firearm, rifle, shotgun, other deadly weapon (including but not limited to knives, clubs, and metal knuckles), dangerous instrument (including items capable of causing death or serious physical injury, when used for that purpose), or ammunition.

Additionally, the Superintendent/Principal is directed to contact local law enforcement, in accordance with the Code of Conduct, district-wide school safety plan, and building-level emergency response plan.

In consultation with the Board of Trustees President and school district attorney, the Superintendent/Principal may designate, in writing, certain other employees at that school to petition the court for the extreme risk protection order. Such employees include: teachers, school guidance counselors, school psychologists, school social workers, school nurse, any other personnel required to hold a teaching or administrative license or certificate, and certain coaches (those who are full- or part-time paid employees required to hold either a temporary coaching license or professional coaching certificate). (Note: Designee…Lead Teacher)

Under Education Law section 3023, the district must defend and indemnify employees against lawsuits for negligence, accidental bodily injury or property damage where the employee is performing his/her duties within the scope of employment.

The Superintendent/Principal or his/her designee is directed to take appropriate steps to notify district staff of the provisions of this policy. This includes ensuring that employees are trained and knowledgeable about when and how to properly utilize the law to best protect the school from violence. Staff will be notified of who is designated to file extreme risk protection orders in the building or district.

Cross-ref:

5300, Code of Conduct

8130, School Safety Plans and Teams

Ref:

Civil Practice Law and Rules Article 63-A

Education Law §3023

Adoption date: 1/15/2020

8131

( ) Required
(X) Local
( ) Notice

PANDEMIC PLANNING

The Board of Trustees recognizes the public's concern over the possibility of a contagious disease outbreak and acknowledges that it is in the best interests of its students, employees and the community to prepare for such a scenario. To this end, the Board directs the Superintendent of Schools to:

1. Implement infection prevention control procedures that could help limit the spread of contagious diseases at schools in the district, including but not limited to:
   - encouraging, through classroom instruction at every grade level and posters, good hygiene habits recommended by public health experts to help protect the school community from contagious diseases (e.g., washing hands frequently with soap and water, coughing/sneezing into tissues or the crook of the elbow instead of one's hand, utilizing alcohol-based/waterless hygiene products and avoiding shaking hands).
   - providing a description of warning signs and symptoms of contagious diseases infections and instruct parents and employees that students and staff displaying such symptoms should not report to school.
   - providing sufficient and accessible infection prevention supplies including soap, alcohol-based/waterless hygiene products, tissues and receptacles for their disposal.
   - following the recommendations of federal, state and local authorities regarding properly cleaning and sanitizing the schools.
   - observing required or recommended social distancing measures (keeping adequate physical space between people as much as possible), utilizing physical barriers, screening people before or during entry to school, and following required or recommended wearing of face coverings.

2. Work with school administrators, district medical personnel, local county health representatives, teachers, guidance counselors, and other staff and parent representatives as appropriate, to prepare, as part of the district's existing emergency/safety plan, a contagious disease preparedness plan. Such plan will include, but not be limited to:

   - Protocols that are substantially consistent with section 27-c of the Labor Law, including: designating essential positions needed to work on-site; telecommuting for non-essential employees; staggered shifts of essential employees; procuring, storing, and accessing personal protective equipment; preventing the spread in the district by those who are exposed to, show symptoms of, or test positive for the disease (including leave available

to employees for testing, treatment, isolation, or quarantine); documenting hours and locations of individuals in order to track the disease and identify those who may have been exposed to the disease; identifying emergency housing for essential employees; and other requirements of the state Department of Health.

- Describing the potential impact of an outbreak on student learning (such as student and staff absences), school closing, school trips, and extracurricular activities based on having various levels of illness among students and staff and the alternative means of delivering education (e.g., educating students through the Internet, long-distance learning, sending assignments home, telephone conference calls, etc.), along with plans to assess student progress once school resumes.
- Establishing procedures for caring for, isolating, and/or transporting students and staff who become ill with contagious diseases while in school, and their return to school after illness.
- Establishing liberal, non-punitive attendance policies for students unique to an outbreak of contagious diseases.
- Developing a process for gathering and analyzing the latest information and recommendations from health experts (for example, from the Centers for Disease Control, the New York State Health Department, the County Health Department, etc.) which will inform district policymakers' decisions.
- Developing a process for communicating information concerning the outbreak of contagious diseases to the school community on a continuing basis. Such efforts may include preparing an information letter for distribution to parents and guardians of students advising them of the dangers of contagious diseases and the steps that may be taken to reduce the risk of infection, and/or establishing a section on the district's website to communicate information about the district's policy concerning contagious diseases and links to relevant governmental websites.
- Coordinating the district's plan with the local and state health departments as well as the State Education Department and area BOCES.
- Assigning responsibility for the activities listed above to appropriate staff.

3. All New York State and federal guidelines related to sick time and absences on the part of the employees will be followed.

In the event that the district implements its emergency plan in response to a pandemic, the Superintendent will keep the Board regularly informed regarding any actions taken and information gathered. The Board may temporarily suspend other policies to the extent necessary to comply with executive orders and other governmental guidance during the pandemic.

Cross-ref: 4765, Remote Learning
5100, Student Attendance
5420, Student Health Services
8130, School Safety Plans and Teams

Adoption date:2/9/21
Amendment date: 8/17/21

8220

( ) Required
(X) Local
( ) Notice

BUILDINGS AND GROUNDS MAINTENANCE AND INSPECTION

To accommodate the district's educational program, the Board of Trustees is committed to providing suitable and adequate facilities. To this end, proper maintenance and inspection procedures are essential. The Board directs the Superintendent of Schools to ensure that proper maintenance and inspection procedures are developed for the school building.

Consistent with federal and state law and regulations, the following items will be included in the district's buildings and grounds maintenance and inspection procedures:

Comprehensive Maintenance Plan

A comprehensive maintenance plan for all the building systems will be instituted to ensure the building is maintained in a state of good repair. Such plan will include provisions for a least toxic approach to integrated pest management and establish maintenance procedures and guidelines which will contribute to acceptable indoor air quality.

Procedures will also be established to ensure the safety of building occupants during maintenance activities including standards for exiting and ventilation, asbestos and lead protocols, noise abatement and control of chemical fumes, gases and other contaminants.

Visual Inspections

A visual inspection of building system components in the school building will take place when required by the State of Commissioner of Education. The inspection report will be made available to the public.

A corrective action plan will be developed by a licensed architect or engineer if a deficiency exists in the building.

Building Condition Surveys

The school and supply building will be assessed every five years by a building condition survey. The survey will be conducted by a team that includes at least one licensed architect or engineer and will include a list of all program spaces and inspection of building system components for evidence of movement, deterioration, structural failure, probable useful life, need for repair and maintenance and need for replacement. Building condition survey reports will be submitted to the Commissioner by January 15th of every fifth year thereafter.

Fire Safety Inspections

An annual inspection for fire and safety hazards will be conducted in accordance with a schedule established by the Commissioner of Education. The inspection will be conducted by a qualified fire inspector and the report will be kept in the district office. Any violation of the State Uniform Fire Prevention and Building Code shall be corrected immediately or within a time frame approved by the Commissioner.

Cross-ref: 7365, Construction Safety
8110, School Building Safety
8115, Pesticides and Pest Management

Ref: 29 CFR §§1910 et seq. (OSHA Hazard Communication)
40 CFR Part 763 (Asbestos Hazard Emergency Response Act)
Education Law §§409-d (Comprehensive Public School Safety Program); 409-e (Uniform Code of Public School Buildings Inspections, Safety Rating and Monitoring); 807-a (Fire Inspections)
Labor Law §§875-883 (toxic substances)
Public Health Law §§4800-4808 (Right to Know, toxic substances)
Environmental Conservation Law §33-0725 (Pesticides)
6 NYCRR Part 325 (Pesticides)
8 NYCRR §§155.1(Educational Facilities); 155.4 (Uniform Code of PublicSchool Buildings Inspection, Safety Rating and Monitoring); 155.8 (Fire and Building Safety Inspections)
9 NYCRR Parts 600-1250 (Uniform Fire Prevention & Building Code)
12 NYCRR Part 56 (Industrial Code Rule concerning asbestos)
Appeal of Anibaldi, 33 Educ. Dep't Rep. 166 (1993) (district required to monitor student's physical symptoms when air quality caused health problems)
Guidelines for the Evaluation and Control of Lead-Based point Hazards in Housing, U.S. Department of Housing and Urban Development, Washington D.C., June 1995)
IPM Workbook for New York State Schools, Cornell Cooperative Extension Community IPM Program with support from New York State Dept. of Environmental Conservation, August 1998

Adoption date: 6/11/13
Amended date: 12/17/15
Amended date: 10/21/21

8330

( ) Required
(X) Local
( ) Notice

AUTHORIZED USE OF SCHOOL-OWNED MATERIALS AND EQUIPMENT

The Board of Trustees permits the use of district-owned materials and equipment (e.g., laptop computers, cell phones, audio-visual equipment, etc.) by Board members, officers, and employees of the district when such material and equipment is needed for district-related purposes.

The Superintendent of Schools shall establish regulations governing the loan and use of such equipment. Such regulations must address:

- the individuals who may properly authorize the use of such material and/or equipment;
- the lack of authority of the borrower to use such material or equipment for private, non-business purposes;
- the responsibilities of the borrower for proper use, care and maintenance;
- that, regardless of condition or other factors, all loaned equipment must be returned to the district. No item may be sold to or purchased by the borrower unless such equipment has been returned to the district for evaluation and, if necessary, disposal in accordance with district policy and procedures.

All equipment shall be inventoried and a list shall be maintained of the date such equipment was loaned, to whom it was loaned, and the date of expected and actual return.

Individuals borrowing district-owned equipment shall be fully liable for any damage or loss occurring to the equipment during the period of its use, and shall be responsible for its safe return. In addition, since Board members, officers and employees are issued district owned equipment in connection with their work responsibilities, the individual using the district owned equipment should not have an expectation of privacy with respect to information contained on the device (e.g., computer files, images, messages).

The District Office shall maintain records of all equipment that is loaned for long-term use (e.g., school year, term of office, etc.) and shall review such list yearly.

<u>Cross-ref:</u> 8332, Use of District Owned Cell Phones
8630, Computer Resources and Data Management

Adoption date: 6/11/13

8332

[ ] Required
[X] Local
[ ] Notice

USE OF DISTRICT-OWNED CELL PHONES

The Board of Trustees recognizes that for purposes of student and staff safety, it is desirable for staff to have access to a cell phone while on a field trip. A cell phone will be provided for this purpose.

The contract for the cell phone shall be secured through the appropriate purchasing process (e.g., competitive bid, RFP process) and shall be subject to review and approval by the Board.

The cell phone is to be used for school district purposes only and other personal use is prohibited. Failure to follow these guidelines may result in discipline of the employee. In addition, since the cell phone is district-owned and issued in connection with their work responsibilities, employees should not have an expectation of privacy with respect to information contained on the device (e.g., text messages, records of phone calls).

As with any district-owned equipment, employees must take proper care of cell phones and take all reasonable precautions against damage, loss, or theft. Any damage, loss, or theft must be reported immediately to the Superintendent of Schools. Since employees are responsible for the safe return of district-owned cell phones, employees who use district-owned cell phones may be liable for damages or loss which occurs during the period of its use.

At least once per year, the Superintendent shall evaluate and report to the Board on the cost and effectiveness of the district's cellular telephone plan.

Ref: Fourth Amendment, U.S. Constitution
Fourteenth Amendment, U.S. Constitution
City of Ontario, California v. Quon, 130 S. Ct. 2619 (2010)

Adoption date: 6/11/13

8334

[ ] Required
[X] Local
[ ] Notice

USE OF DISTRICT CREDIT CARDS

The Board of Trustees permits the use of a district credit/debit card by the District Clerk and District Treasurer to pay for actual and necessary expenses incurred in the performance of work-related duties for the district. The credit card will be in the name of the school district.

The Board shall ensure that the credit card is secured through an RFP process and the relationship between the district and the credit card company is such that the district preserves its right to refuse to pay any claim or portion thereof that is not expressly authorized, does not constitute a proper district charge, or supersedes any laws, rules, regulations, or policies otherwise applicable. In addition, the Board will ensure that no claim shall be paid unless an itemized voucher approved by the officer whose action gave rise or origin to the claim, shall have been presented to the Board and shall have been audited and allowed.

Credit cards may only be used for legitimate school district business expenditures. The use of credit cards is not intended to circumvent the district's policy on purchasing. Credit cards may be used when the vendor does not accept purchase orders (e.g., online vendors where the item is not readily available elsewhere or in time-sensitive instances.)

The user must take proper care of these credit cards and take all reasonable precautions against damage, loss, or theft. Any damage, loss, or theft must be reported immediately to the Business Official and to the appropriate financial institution. Failure to take proper care of credit cards or failure to report damage, loss or theft may subject the employee to financial liability.

Purchases that are unauthorized, illegal, represent a conflict of interest, are personal in nature or violate the intent of this policy may result in credit card revocation and discipline of the employee.

The user must submit detailed documentation, including itemized receipts for commodities, services, travel and/or other actual and necessary expenses which have been incurred in connection with school-related business for which the credit card has been used.

The Superintendent shall periodically, but no less than twice a year, monitor the use of each credit card and report any serious problems and/or discrepancies directly to the Board.

Cross-ref: 6700, Purchasing
6830, Expense Reimbursement

Ref: Opns. St. Compt. No. 79-202 (use of multi-purpose credit cards by municipal employees)
Opns. St. Compt. No. 79-494
Opns. St. Compt. No. 78-897 (gas credit cards)

Adoption date: 6/11/13

8410
[ ] Required
[X] Local
[ ] Notice

STUDENT TRANSPORTATION

The Board of Trustees affirms its goal of providing a safe and economical transportation system for district students. Transportation shall be provided at district expense to those students who are eligible as authorized by the Board.

The major objectives in the management of the student transportation program shall include the following:

1. to provide efficient, effective and safe service;
2. to ensure that all students whose disability or distance from school requires them to receive necessary transportation do, in fact, receive it;
3. to adapt the system to the demands of the instructional program;
4. to review at least once a year school bus schedules and routing plans to ensure that maximum efficiency and safety are maintained; and
5. to review at least once a year the eligibility for transportation of students residing in the district, to ensure that all entitled to the services receive them.

The Superintendent of Schools shall be responsible for administering the transportation program through a contract with an outside company. The program shall comply with all applicable laws, regulations and policies established by federal, state and local authorities.

The Superintendent shall work with the transportation company to establish bus routes. Authorized bus stops shall be located at convenient intervals in places where students may embark and disembark the buses, and await the arrival of buses, in the utmost safety allowed by road conditions.

The Board of Trustees also recognizes that, as per New York State Education Law, the District does not have the obligation to transport its resident students who live more than fifteen (15) miles from their private school of attendance.

Ref: Education Law §§305(14); 1501-b; 1807; 3602(7); 3623; 3635 et seq.
Matter of Handicapped Child, 24 EDR 41 (1984)
Matter of Zakrezewski, 22 EDR 381 (1983)
Matter of Nowak, 22 EDR 91 (1982)
Matter of Fox, 19 EDR 439 (1980)

Adoption date: 6/11/13
Amended date: 12/17/15

8414.5

[ ] Required
[X] Local
[x] Notice

ALCOHOL AND DRUG TESTING OF BUS DRIVERS

The Board of Trustees recognizes the dangers inherent in alcohol and controlled substance use, especially use by school bus drivers. Although the district contracts with an outside company to provide transportation services to students, the Board understands the requirement for that company to follow all applicable state and federal laws and regulations concerning alcohol and drug testing of bus drivers. All contracts for student transportation will contain the requirements that: (1) the transportation company will comply with the requirement to adequately and appropriately test its drivers for alcohol and drug use, and that (2) the transportation company will certify that it does so.

Adoption date: 12/11/12

8630
[ ] Required
[X] Local
[ ] Notice

COMPUTER RESOURCES AND DATA MANAGEMENT

The Board of Trustees recognizes that computers are a powerful and valuable education and research tool and as such are an important part of the instructional program. In addition, the district depends upon computers as an integral part of administering and managing the schools' resources, including the compilation of data and recordkeeping for personnel, students, finances, supplies and materials. This policy outlines the Boards expectations in regard to these different aspects of the district's computer resources.

General Provisions

The Superintendent shall be responsible for designating a Chief Information Officer who will oversee the use of district computer resources. The Superintendent working in concert with the Chief Information Officer and Head Teacher will prepare in-service programs for the training and development of district staff in computer skills, appropriate use of computers and for the incorporation of computer use in subject areas.

The Superintendent, working in conjunction with the designated purchasing agent for the district, will be responsible for the purchase and distribution of computer software and hardware throughout the schools. They shall prepare and submit for the Board's approval a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or district needs.

The Superintendent, working with the Chief Information Officer, shall establish regulations governing the use and security of the district's computer resources (computer resources include all devices that process data, including but not limited to, laptops, fax machines, copiers and scanners). The security and integrity of the district computer network and data is a serious concern to the Board and the district will make every reasonable effort to maintain the security of the system. All users of the district's computer resources shall comply with this policy and regulation, as well as the district's policy 4526, Computer Use in Instruction. Failure to comply may result in disciplinary action, as well as suspension and/or revocation of computer access privileges.

All users of the district's computer resources must understand that use is a privilege, not a right, and that use entails responsibility. Users of the district's computer network must not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any use of the district's computer network. The district

reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's computer network.

Management of Computer Records

The Board recognizes that since district data is managed by computer, it is critical to exercise appropriate control over computer records, including financial, personnel and student information. The Superintendent, working with the Chief Information Officer and the district's business official, shall establish procedures governing management of computer records.

- passwords,
- system administration,
- separation of duties,
- remote access,
- encryption,
- user access and permissions appropriate to job titles and duties,
- disposal of computer equipment and resources (including deleting district data or destroying the equipment),
- inventory of computer resources (including hardware and software),
- data back-up (including archiving of e-mail),
- record retention, and
- disaster recovery plans and notification plans.

If the district contracts with a third-party vendor for computing services, the Superintendent, in consultation with the Chief Information Officer or the District Treasurer will ensure that all agreements address the procedures listed above, as applicable.

Review and Dissemination

Since computer technology is a rapidly changing area, it is important that this policy be reviewed periodically by the Board. The regulation governing appropriate computer use will be distributed annually to staff and students and will be included in both employee and student handbooks.

Cross-ref: 1120, School District Records
4526, Computer Use for Instruction
4526.1, Internet Safety
5500, Student Records
6600, Fiscal Accounting and Reporting
6700, Purchasing
6900, Disposal of District Property
8635, Information Security Breach and Notification

Adoption date: 2/12/13
Amended: 4/21/16

8630-R

COMPUTER RESOURCES AND DATA MANAGEMENT REGULATION

The following rules and regulations govern the use of the district's computer network system, employee access to the Internet, and management of computerized records.

I. Administration

- The Superintendent of Schools shall designate a computer network coordinator to oversee the district's computer network.
- The computer network coordinator shall monitor and examine all network activities, as appropriate, to ensure proper use of the system. The Chief Information Officer shall maintain an updated inventory of all computer hardware and software resources.
- The computer network coordinator shall develop and implement procedures for data back-up and storage. These procedures will facilitate the disaster recovery and notification plan and will comply with the requirements for records retention in compliance with the district's policy on School District Records (1120).
- The computer network coordinator shall be responsible for disseminating and interpreting district policy and regulations governing use of the district's network at the building level with all network users.
- The computer network coordinator shall provide employee training for proper use of the network and will ensure that staff supervising students using the district's network provide similar training to their students, including providing copies of district policy and regulations (including policy 4526, Computer Use in Instruction) governing use of the district's network.
- The computer network coordinator shall take reasonable steps to protect the network from viruses, other software, and network security risks that would compromise the network or district information.
- All student and employee agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the district office.
- Consistent with applicable internal controls, the Superintendent in conjunction with the school business official and the computer network coordinator, will ensure the proper segregation of duties in assigning responsibilities for computer resources and data management.

II. Internet Access

Student Internet access is addressed in policy and regulation 4526, Computer Use in Instruction. District employees and third party users are governed by the following regulations:

- Employees will be issued an e-mail account through the district's computer network.
- Employees are expected to review their e-mail daily.
- Communications with parents and/or students should be saved as appropriate and the district will archive the e-mail records according to procedures developed by the computer network coordinator.
- Employees may access the internet for education-related and/or work-related activities.
- Employees shall refrain from using computer resources for personal use.

- Employees are advised that they must not have an expectation of privacy in the use of the district's computers.
- Use of computer resources in ways that violate the acceptable use and conduct regulation, outlined below, will be subject to discipline.

III. Acceptable Use and Conduct

The following regulations apply to all staff and third party users of the district's computer system:

- Access to the district's computer network is provided solely for educational and/or research purposes and management of district operations consistent with the district's mission and goals.
- Use of the district's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users will be issued a login name and password. Passwords must be changed periodically and must be of sufficient complexity as determined by the district.
- Only those network users with permission from the Superintendent or computer network coordinator may access the district's system from off-site (e.g., from home).
- All network users are expected to take reasonable precaution to secure district information stored on devices they use, including maintaining responsible custody over computer resources, ensuring no unauthorized use of district devices, and exercising prudent judgement when browsing the internet and opening email.
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the district's network must notify appropriate staff. Any network user identified as a security

risk or having a history of violations of district computer use guidelines may be denied access to the district's network.

IV. Prohibited Activity and Uses

The following is a list of prohibited activity for all staff and third party users concerning use of the district's computer network. Any violation of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the district computer network.
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Use of another's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy district equipment or materials, data of another user of the district's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus, malware on the network, and not reporting security risks as appropriate.
- Using the network to send anonymous messages or files.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software, using personal disks, or downloading files on the district's computers and/or network without the permission of the appropriate district official or employee.
- Using district computing resources for fraudulent purposes or financial gain. Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- Wastefully using finite district resources.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or employee.
- Using the network while your access privileges are suspended or revoked.

- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.
- Exhibiting careless behavior with regard to information security (e.g., sharing or displaying passwords, leaving computer equipment unsecured or unattended, etc.).

V. No Privacy Guarantee

Users of the district's computer network should not expect, nor does the district guarantee, privacy for electronic mail (e-mail) or any use of the district's computer network. The district reserves the right to access and view any material stored on district equipment or any material used in conjunction with the district's computer network.

VI. Sanctions

All users of the district's computer network and equipment are required to comply with the district's policy and regulations governing the district's computer network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

VII. District Responsibilities

The district makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the district assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the district's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information.

The district will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the user's own negligence or any other errors or omissions. The district also will not be responsible for unauthorized financial obligations resulting from the use of or access to the district's computer network or the Internet.

The district will take reasonable steps to protect the information on the network and provide a secure network for data storage and use, including ensuring that contracts with vendors address data security issues and that district officials provide appropriate oversight. Disposal of district computer resources shall ensure the complete removal of district information, or the secure destruction of the resource. Even though the district may use technical and/or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the district policy and regulation.

Adoption date: 4/21/16

8635

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

INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION

The Board of Trustees acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. The Board adopts the National Institute for Standards and Technology Cybersecurity Framework Version 1.1 (NIST CSF) for data security and protection. The Superintendent and/or designee or Data Privacy Officer is responsible for ensuring the district's systems follow NIST CSF and adopt technologies, safeguards and practices which align with it. This will include an assessment of the district's current cybersecurity state, their target future cybersecurity state, opportunities for improvement, progress toward the target state, and communication about cyber security risk.

The Board will designate a Data Protection Officers to be responsible for the implementation of the policies and procedures required in Education Law §2-d and its accompanying regulations, and to serve as the point of contact for data security and privacy for the district. (This appointment will be made at the annual organizational meeting)

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, and the Data Protection Officer (where applicable) to establish regulations which address:

- the protections of "personally identifiable information" of student and teachers/principal under Education Law §2-d and Part 121 of the Commissioner of Education;
- the protections of "private information" under State Technology Law §208 and the NY SHIELD Act; and
- procedures to notify persons affected by breaches or unauthorized access of protected information.

I. Student and Teacher/Principal "Personally Identifiable Information" under Education Law §2-d

A. General Provisions

PII as applied to student data is as defined in Family Educational Rights and Privacy Act (Policy 5500), which includes certain types of information that could identify a student, and is listed in the accompanying regulation 8635-R. PII as applied to teacher and principal data, means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

In accordance with Education Law § 2-d(b)(1) and Section 121.5 of the Regulations of the Commissioner of Education, disclosure of personally identifiable information from the student records of [the District/BOCES], including directory information, to individuals or entities other than the parent/guardian or eligible student or which is not otherwise permitted by applicable consent or provision of Education Law § 2-d, shall be predicated upon a determination that the proposed use would benefit students and [the District/BOCES] (e.g., improve academic achievement, empower parents and students with information, and/or advance efficient and effective school operations).

The district will protect the confidentiality of student and teacher/principal PII while stored or transferred using industry standard safeguards and best practices, such as encryption, firewalls, and passwords. The district will monitor its data systems, develop incident response plans, limit access to PII to district employees and third-party contractors who need such access to fulfill their professional responsibilities or contractual obligations, and destroy PII when it is no longer needed.

Certain federal laws and regulations provide additional rights regarding confidentiality of and access to student records, as well as permitted disclosures without consent, which are addressed in policy and regulation 5500, Student Records.

Under no circumstances will the district sell PII. It will not disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by any other party for any marketing or commercial purpose, or permit another party to do so. Further, the district will take steps to minimize the collection, processing, and transmission of PII.

Except as required by law or in the case of enrollment data, the district will not report the following student data to the State Education Department:

1. juvenile delinquency records;
2. criminal records;
3. medical and health records; and
4. student biometric information.

The district has created and adopted a Parent's Bill of Rights for Data Privacy and Security (see Exhibit 8635-E). It has been published on the district's website at www.sagaponackschool.com and can be requested from the district clerk.

B. Third-party Contractors

The district will ensure that contracts with third-party contractors reflect that confidentiality of any student and/or teacher or principal PII be maintained in accordance with federal and state law and the district's data security and privacy policy.

Each third-party contractor that will receive student data or teacher or principal data must:

1. adopt technologies, safeguards and practices that align with the NIST CSF;

2. comply with the district's data security and privacy policy and applicable laws impacting the district;
3. limit internal access to PII to only those employees or sub-contractors that need access to provide the contracted services;
4. not use the PII for any purpose not explicitly authorized in its contract;
5. not disclose any PII to any other party without the prior written consent of the parent or eligible student (i.e., students who are eighteen years old or older):
    a. except for authorized representatives of the third-party contractor to the extent they are carrying out the contract; or
    b. unless required by statute or court order and the third-party contractor provides notice of disclosure to the district, unless expressly prohibited.
6. maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of PII in its custody;
7. use encryption to protect PII in its custody; and
8. not sell, use, or disclose PII for any marketing or commercial purpose, facilitate its use or disclosure by others for marketing or commercial purpose, or permit another party to do so. Third party contractors may release PII to subcontractors engaged to perform the contractor's obligations, but such subcontractors must abide by data protection obligations of state and federal law, and the contract with the district.

If the third-party contractor has a breach or unauthorized release of PII, it will promptly notify the district in the most expedient way possible without unreasonable delay but no more than seven calendar days after the breach's discovery.

C. Third-Party Contractors' Data Security and Privacy Plan

The district will ensure that contracts with all third-party contractors include the third-party contractor's data security and privacy plan. This plan must be accepted by the district.

At a minimum, each plan will:

1. outline how all state, federal, and local data security and privacy contract requirements over the life of the contract will be met, consistent with this policy;
2. specify the safeguards and practices it has in place to protect PII;
3. demonstrate that it complies with the requirements of Section 121.3(c) of this Part;
4. specify how those who have access to student and/or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;
5. specify if the third-party contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;
6. specify how the third-party contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the district;

7. describe if, how and when data will be returned to the district, transitioned to a successor contractor, at the district's direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires.

D. Training

The district will provide annual training on data privacy and security awareness to all employees who have access to student and teacher/principal PII.

E. Reporting

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of student or teacher/principal PII maintained by the district will be promptly reported to the Data Protection Officer, the Superintendent and the Board of Education.

F. Notifications

The Data Privacy Officer will report every discovery or report of a breach or unauthorized release of student, teacher or principal PII to the State's Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

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 or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation or cause further disclosure of PII by disclosing an unfixed security vulnerability, 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.

The Superintendent, in consultation with the Data Protection Officer, will establish procedures to provide notification of a breach or unauthorized release of student, teacher or principal PII, and establish and communicate to parents, eligible students, and district staff a process for filing complaints about breaches or unauthorized releases of student and teacher/principal PII.

II. "Private Information" under State Technology Law §208

"Private information" is defined in State Technology Law §208, and includes certain types of information, outlined in the accompanying regulation, which would put an individual at risk for

identity theft or permit access to private accounts. "Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation.

Any breach of the district's information storage or computerized data which compromises the security, confidentiality, or integrity of "private information" maintained by the district must be promptly reported to the Superintendent and the Board of Trustees.

The Board directs the Superintendent of Schools, in accordance with appropriate business and technology personnel, to establish regulations which:

- Identify and/or define the types of private information that is to be kept secure;
- Include procedures to identify any breaches of security that result in the release of private information; and
- Include procedures to notify persons affected by the security breach as required by law.

III. Employee "Personal Identifying Information" under Labor Law § 203-d

Pursuant to Labor Law §203-d, the district will not communicate employee "personal identifying information" to the general public. This includes:

1. social security number;
2. home address or telephone number;
3. personal email address;
4. Internet identification name or password;
5. parent's surname prior to marriage; and
6. drivers' license number.

In addition, the district will protect employee social security numbers in that such numbers will not be:

1. publicly posted or displayed;
2. visibly printed on any ID badge, card or time card;
3. placed in files with unrestricted access; or
4. used for occupational licensing purposes.

Employees with access to such information will be notified of these prohibitions and their obligations.

Cross-ref:
1120, District Records
5500, Student Records
8630, Computer Resources and Data Management
Ref:
State Technology Law §§201-208
Labor Law §203-d
Education Law §2-d
8 NYCRR Part 121

SAGAPONACK

Adoption date: 12/11/12
Amended date: 3/17/21
Amended date: 1/18/22

8635-R

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

INFORMATION AND DATA PRIVACY, SECURITY, BREACH AND NOTIFICATION

This regulation addresses information and data privacy, security, breach and notification requirements for student and teacher/principal personally identifiable information under Education Law §2-d, as well as private information under State Technology Law §208.

The district will inventory its computer programs and electronic files to determine the types of information that is maintained or used by the district, and review the safeguards in effect to secure and protect that information.

I. Student and Teacher/Principal "Personally Identifiable Information" under Education Law §2-d

A. Definitions

"*Biometric record*," as applied to student PII, means one or more measurable biological or behavioral characteristics that can be used for automated recognition of person, which includes fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting.

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

"*Disclose*" *or Disclosure* means to permit access to, or the release, transfer, or other communication of PII by any means, including oral, written, or electronic, whether intended or unintended.

"*Personally Identifiable Information*" (PII) as applied to students means the following information for district students:

1. the student's name;
2. the name of the student's parent or other family members;
3. the address of the student or student's family;
4. a personal identifier, such as the student's social security number, student number, or biometric record;
5. other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6. other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have

personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

7. information requested by a person who the district reasonably believes knows the identity of the student to whom the education record relates.

"*Personally Identifiable Information*" (PII) as applied to teachers and principals means results of Annual Professional Performance Reviews that identify the individual teachers and principals, which are confidential under Education Law §§3012-c and 3012-d, except where required to be disclosed under state law and regulations.

"*Third-Party Contractor*" means any person or entity, other than an educational agency (i.e., a school, school district, BOCES or State Education Department), that receives student or teacher/principal PII from the educational agency pursuant to a contract or other written agreement for purposes of providing services to such 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 includes an educational partnership organization that receives student and/or teacher/principal PII from a school district to carry out its responsibilities pursuant to Education Law §211-e (for persistently lowest-achieving schools or schools under registration review) and is not an educational agency. This also includes a not-for-profit corporation or other nonprofit organization, other than an educational agency.

B. Complaints of Breaches or Unauthorized Releases of PII

If a parent/guardian, eligible student, teacher, principal or other district employee believes or has evidence that student or teacher/principal PII has been breached or released without authorization, they must submit this complaint in writing to the district. Complaints may be received by the Data Privacy Officer, but may also be received by any district employee, who must immediately notify the Data Privacy Officer. This complaint process will be communicated to parents, eligible students, teachers, principals, and other district employees.

The district will acknowledge receipt of complaints promptly, commence an investigation, and take the necessary precautions to protect personally identifiable information.

Following its investigation of the complaint, the district will provide the individual who filed a complaint with its findings within a reasonable period of time. This period of time will be no more than 60 calendar days from the receipt of the complaint.

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

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, including the Records Retention and Disposition Schedule ED-1.

C. Notification of Student and Teacher/Principal PII Breaches

If a third-party contractor has a breach or unauthorized release of PII, it will promptly notify the Data Privacy Officer or Superintendent in the most expedient way possible, without unreasonable delay, but no more than seven calendar days after the breach's discovery.

The Data Privacy Officer or Superintendent will then notify the State Chief Privacy Officer of the breach or unauthorized release no more than 10 calendar days after it receives the third-party contractor's notification using a form or format prescribed by the State Education Department.

The Data Privacy Officer or Superintendent will report every discovery or report of a breach or unauthorized release of student, teacher or principal data to the Chief Privacy Officer without unreasonable delay, but no more than 10 calendar days after such discovery.

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 or third-party contractor notification.

However, if notification would interfere with an ongoing law enforcement investigation or cause further disclosure of PII by disclosing an unfixed security vulnerability, 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 brief description of the breach or unauthorized release,
- the dates of the incident and the date of discovery, if known;
- a description of the types of PII affected;
- an estimate of the number of records affected;
- a brief description of the district's investigation or plan to investigate; and
- contact information for representatives who can assist parents or eligible students with additional questions.

Notification must 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 will pay for or promptly reimburse the district for the full cost of such notification.

The unauthorized acquisition of student social security numbers, student ID numbers, or biometric records, when in combination with personal information such as names or other identifiers, may also constitute a breach under State Technology Law §208 if the information is not encrypted, and the acquisition compromises the security, confidentiality, or integrity of personal information maintained by the district. In that event, the district is not required to notify affected people twice, but must follow the procedures to notify state agencies under State Technology Law §208 outlined in section II of this regulation.

II. "Private Information" under State Technology Law §208

A. Definitions

"*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 personal information plus the data element is not encrypted or encrypted with an encryption key that has also been accessed or acquired:

- Social security number;
- Driver's license number or non-driver identification card number;
- 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;
- account number or credit or debit card number, if that number could be used to access a person's financial account without other information such as a password or code; or
- biometric information (data generated by electronic measurements of a person's physical characteristics, such as fingerprint, voice print, or retina or iris image) used to authenticate or ascertain a person's identity; or

2. A user name or email address, along with a password, or security question and answer, that would permit access to an online account.

"Private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;

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

B. Procedure for Identifying Security Breaches

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, the district will consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as removal of lost or stolen computer, or other device containing information;
2. indications that the information has been downloaded or copied;
3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; and/or
4. any other factors which the district shall deem appropriate and relevant to such determination.

C. Notification of Breaches to Affected Persons

Once it has been determined that a security breach has occurred, the district will take the following steps:

1. If the breach involved computerized data *owned or licensed* by the district, the district will notify those New York State residents 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 to restore the integrity of the 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.
2. If the breach involved computer data *maintained* by the district, the district will notify the owner or licensee of the information of the breach 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 required notice will include (a) district contact information, (b) a description of the categories/information that were or are reasonably believed to have been accessed or acquired without authorization, (c) which specific elements of personal or private information were or are reasonably believed to have been acquired and (d) the telephone number and website of relevant state and federal agencies that provide information on security breach response and identity theft protection and prevention. This notice will be directly provided to the affected individuals by either:

1. Written notice
2. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving the notice in electronic form; and that the district keeps a log of

each such electronic notification. In no case, however, will the district require a person to consent to accepting such notice in electronic form as a condition of establishing a business relationship or engaging in any transaction.

3. Telephone notification, provided that the district keeps a log of each such telephone notification.

However, if the district can demonstrate to the State Attorney General that (a) the cost of providing notice would exceed $250,000; or (b) that the number of persons to be notified exceeds 500,000; or (c) that the district does not have sufficient contact information, substitute notice may be provided. Substitute notice would consist of all of the following steps:

1. E-mail notice when the district has such address for the affected individual;
2. Conspicuous posting on the district's website, if they maintain one; and
3. Notification to major media.

However, the district is not required to notify individuals if the breach was inadvertently made by individuals authorized to access the information, and the district reasonably determines the breach will not result in misuse of the information, or financial or emotional harm to the affected persons. The district will document its determination in writing and maintain it for at least five years, and will send it to the State Attorney General within ten days of making the determination.

Additionally, if the district has already notified affected persons under any other federal or state laws or regulations regarding data breaches, including the federal Health Insurance Portability and Accountability Act, the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, or New York State Education Law §2-d, it is not required to notify them again. Notification to state and other agencies is still required.

D. Notification to State Agencies and Other Entities

Once notice has been made to affected New York State residents, the district shall notify the State Attorney General, the State Department of State, and the State Office of Information Technology Services as to the timing, content, and distribution of the notices and approximate number of affected persons.

If 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 the approximate number of affected individuals. A list of consumer reporting agencies will be furnished, upon request, by the Office of the State Attorney General.

If the district is required to notify the U.S. Secretary of Health and Human Services of a breach of unsecured protected health information under the federal Health Insurance Portability and Accountability Act (HIPAA) or the federal Health Information Technology for Economic and Clinical Health (HI TECH) Act, it will also notify the State Attorney General within five business days of notifying the Secretary.

Adoption date:3/17/21

8635-E

PARENTS' BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY

The Sagaponack Common School District, in recognition of the risk of identity theft and unwarranted invasion of privacy, affirms its commitment to safeguarding student personally identifiable information (PII) in educational records from unauthorized access or disclosure in accordance with State and Federal law. The Sagaponack Common School District establishes the following parental bill of rights:

- Student PII will be collected and disclosed only as necessary to achieve educational purposes in accordance with State and Federal Law.

- The district and third-party contractors and subcontractors, will not sell student PII or use or disclose it for any marketing or commercial purposes or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so;

- Parents have the right to inspect and review the complete contents of their child's education record.

- State and federal laws, such as NYS Education Law §2-d and the Family Educational Rights and Privacy Act, protect the confidentiality of students' personally identifiable information. Safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred;

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

- Parents have the right to have complaints about possible breaches and unauthorized disclosures of student data addressed. Complaints should be directed to (The Superintendent- *Sagaponack Common School District PO Box 1500 Sagaponack, NY 11962, (631) 537-0651 or email super1@sagaponackschool.org* . Complaints can also be directed to the New York State Education Department online at http://nysed.gov/data-privacy-security/report-improper-disclosure, by mail to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234 or by email to privacy@nysed.gov or by telephone at 518-474-0937.

- Parents have the right to be notified in accordance with applicable laws and regulations if a breach or unauthorized release of their student's PII occurs.

- All district and school employees and officers with access to PII will receive annual training on applicable federal and state laws, regulations, district and school policies and safeguards which will be in alignment with industry standards and best practices to protect PII.

- In the event that the District engages a third party provider to deliver student educational services, the contractor or subcontractors will be obligated to adhere to State and Federal Laws to safeguard student PII. Parents can request information about third party contractors by contacting The Sagaponack Common School District, PO Box 1500 Sagaponack, NY 11962, (631) 537-0651 or by emailing the Superintendent at super1@sagaponackschool.org or can access the information on the district's website: www.sagaponackschool.com.

PARENT BILL OF RIGHTS FOR STUDENT DATA PRIVACY AND SECURITY THIRD PARTY CONTRACTOR SUPPLEMENT

The (*insert name of contractor*) has been engaged by the Sagaponack Common School District to provide services. In this capacity, the company may collect, process, manage, store or analyze student or teacher/principal personally identifiable information (PII).

The (*insert name of contractor*) will provide the district with (*describe specific purpose for which the PII will be used*).

The (*insert the name of contractor*) will ensure that subcontractors or others that the company shares PII will abide by data protection and security requirements of district policy, and state and federal law and regulations by (*describe methods/procedures to safeguard data use by subcontractors*).

PII will be stored (*describe the location in a manner that protects data security*).

Parents may challenge the accuracy of PII held by (*insert name of contractor*) by contacting The Sagaponack Common School District, PO Box 1500 Sagaponack, NY 11962, (631) 537-0651 or by emailing the Superintendent at super1@sagaponackschool.org (*insert contact information, including title, phone number, mailing address and email address*).

The (*insert name of contractor*) will take reasonable measures to ensure the confidentiality of PII by implementing the following (*describe the following, as applicable*):

- Password protections
- Administrative procedures

- Encryption while PII is in motion and at rest
- Firewalls

The contractor's agreement with the district begins on (*insert date*) and ends on (*insert date*). Once the contractor has completed its service to the district, records containing student PII will

be (*select one*: destroyed or returned) by (*insert date*) via the following (insert method if destroyed or format if returned).

Adoption date: 3/17/21
Amended date: 10/21/21