POLICY

No. 8130

School Safety Plans and Teams

WESTBURY UNION FREE SCHOOL DISTRICT
BOARD OF EDUCATION

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 Education 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 shall 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 shall be designed to prevent or minimize the effects of serious violent incidents and emergencies and to facilitate the district's coordination with local and county resources. The plans shall also address risk reduction/prevention, response and recovery with respect to a variety of types of emergencies and violent incidents in district schools.

In accordance with state law and regulation, the district shall 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 shall annually appoint a district-wide school safety team that includes, but is not be limited to, a representative from the following constituencies: the Board, students, teachers, administrators, and parent organizations, school safety personnel and other school personnel. This team shall be responsible for the development and annual review of the comprehensive district-wide school safety plan. The plan shall cover all district school buildings and shall 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 shall include all those elements required by law and regulation.

Building-level safety team and emergency response plans

Each Building Principal shall be responsible for annually appointing a school safety team that includes representation from teachers, administrators, parent organizations, school safety personnel, other school personnel, local law enforcement officials, local ambulance and other emergency response agencies. The school safety team shall be responsible for the development and review of a building-level emergency response plan for each district building. The plan(s) shall address communication, emergency response (including insuring that local responders have access to floor plans, blueprints, and other appropriate maps of school property and the immediate surrounding area), and evacuation at the building level and shall include all components required by law and regulation.

Within each building, the school safety team shall designate:

- an emergency response team that includes appropriate school personnel, local law enforcement officials and representatives from local, regional and/or state emergency response agencies to assist the school community in responding to a serious 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.

The Building Principal, in consultation with the Superintendent, shall 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 shall be composed of, but not limited to, the following personnel from both within the school and the larger community, as appropriate: building administrators, the medical director and/or school nurse, school counselors, local mental health and social service providers, law enforcement, school resource officers, security personnel, and facilities and maintenance personnel in consultation with legal counsel. The team shall meet regularly. The team shall be mindful of the need for discretion and observance of confidentiality requirements.

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

The Building Principal shall 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. A summary of the building-level plan will be made available for public inspection.

Annual Review and Report

All plans shall be reviewed and updated, if necessary, by the appropriate safety team by May 15th every year. In conducting the review, the teams shall 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 shall remain in effect. If the district-wide plan requires change, then the updated plan shall be submitted to the Board of Education 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. If the building-level plan requires change, a summary of it will be made available for public comment and public hearing. All plans must be adopted by the Board of Education by July 1.

The Superintendent of Schools shall be responsible for filing the district-level school safety plan and any amendments to the plan with the Commissioner within 30 days after their adoption. The district-wide plan will be posted on the district's website. Each Building Principal shall be responsible for filing the building-level safety plan for his or her building and any amendments to the plan with the appropriate local law enforcement agency and the state police within 30 days after their adoption.

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: July 17, 2014

POLICY

No. 8414.6

Idling School Buses on School Grounds

WESTBURY UNION FREE SCHOOL DISTRICT
BOARD OF EDUCATION

IDLING SCHOOL BUSES ON SCHOOL GROUNDS

The Board of Education recognizes the need to promote the health and safety of District students and staff and to protect the environment from harmful emissions found in bus and vehicle exhaust. In accordance with Education Law and Commissioner's Regulations, the District will minimize, to the extent practicable, the idling of all school buses and other vehicles owned or leased by the District while such bus or vehicle is parked or standing on school grounds or in the front of any school. This policy also applies to contractor owned and operated school buses under contract with the District. The District shall ensure that each driver of a school bus or other vehicle owned, leased or contracted for by the District turn off the engine of the bus or vehicle while waiting for passengers to load or off load on school grounds, or while such vehicle is parked or standing on school grounds or in front of or adjacent to any school.

Exceptions

Unless otherwise required by State or local law, the idling of a school bus or vehicle engine may be permitted to the extent necessary to achieve the following purposes:

a) For mechanical work; or
b) To maintain an appropriate temperature for passenger comfort; or
c) In emergency evacuations where necessary to operate wheelchair lifts.

Private Vendor Transportation Contracts

All contracts for pupil transportation services between the School District and a private vendor that are entered into on or after August 21, 2008, shall include a provision requiring such vendor's compliance with the provisions of reducing idling in accordance with Commissioner's Regulations Section 156.3(h).

Education Law Section 3637
Vehicle and Traffic Law Section 142
8 New York Code of Rules and Regulations (NYCRR) Section 156.3(h)

Adoption date: January 22, 2015

POLICY

No. 8505

Meal Charge and Prohibition Against Meal Shaming

WESTBURY UNION FREE SCHOOL DISTRICT
BOARD OF EDUCATION

Meal Charge and Prohibition Against Meal Shaming Policy

I. Purpose

The goal of the Westbury UFSD is to provide student access to nutritious no- or low-cost meals each school day and to ensure that a pupil whose parent/guardian has unpaid school meal fees is not shamed or treated differently than a pupil whose parent/guardian does not have unpaid meal fees.

Unpaid charges place a large financial burden on our school. The purpose of this policy is to insure compliance with federal requirements for the USDA Child Nutrition Program and, 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 Westbury UFSD 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. The Westbury UFSD provides this policy as a courtesy to those students in the event that they forget or lose their money. Charging of items outside of the reimbursable meals (a la carte items, adult meals, etc.) is expressly prohibited.

II. Policy

Free Meal Benefit - Free 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.

Reduced Meal Benefit - Reduced eligible students will be allowed to receive a breakfast of their choice for $*0.25* and lunch of their choice for $*0.25* 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 school to withhold a meal. A la carte items or other similar items must be paid/prepaid.

Full Pay Students - Students will pay for meals at the school'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 school to withhold a meal. A la carte items or other similar items must be paid/prepaid.

ONGOING STAFF TRAINING:

- Staff will be trained annually and throughout the year as needed on the procedures for managing meal charges using the NYSED Webinar or the school's training program.

- Staff training includes 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 meal charges within 14 days of the charge and then every 14 days thereafter.

PARENT OUTREACH:

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

- School 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.

- School 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 child to have insufficient funds, offering any other assistance that is appropriate.

MINIMIZING STUDENT DISTRESS:

- School will not publicly identify or stigmatize any student on the line or discuss any outstanding meal debt in the presence of any other students.

- Students who incur meal charges will not be required to wear a wristband or handstamp, or to do chores or work to pay for meals.

- Schools 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 meal charges.

- Schools will not take any action directed at a pupil to collect unpaid school meal fees.

- Schools will deal directly with parents/guardians regarding unpaid school meal fees.

ONGOING ELIGIBILITY CERTIFICATION:

- School staff will conduct direct certification with NYSSIS or using NYSED Roster Upload to maximize free eligibility. NYSED provides updated direct certification data monthly.

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

- Schools using electronic meal application will provide an explanation of the process in the school enrollment packet and instructions on how to request a paper application at no cost.

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

- Schools will use administrative prerogative judiciously, only after using exhaustive efforts to obtain a completed application from the parent/guardian only with available information on family size and income that falls within approvable guidelines.

- Schools will coordinate with the foster, homeless, migrant, runaway coordinators to certify eligible students. School liaisons required for homeless, foster, and migrant students shall coordinate with the nutrition department to make sure such students receive free school meals, in accordance with federal law.

Students/Parents/Guardians may pay for meals in advance via www.westburyschools.org or with a check payable to *Westbury UFSD Child Nutrition Fund*. Further details are available by calling 516-874-1146. Funds should be maintained in accounts to minimize the possibility that a child 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.

Refunds for withdrawn, and graduating students; a written or e-mailed request for a refund of any money remaining in their account must be submitted. Students who are graduating at the end of the year will be given the option to transfer to a sibling's account with a written request.

Unclaimed Funds must be requested within one school year. Unclaimed funds will then become the property of the *Westbury UFSD Child Nutrition Program.*

Adoption date: August 16, 2018

POLICY

No. 8630

Computer Resources and Data Management

WESTBURY UNION FREE SCHOOL DISTRICT
BOARD OF EDUCATION

COMPUTER RESOURCES AND DATA MANAGEMENT

The Board of Education 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 Director of Technology who will oversee the use of district computer resources. The Director of Technology 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, and the Assistant Superintendent for Curriculum, Instruction and Personnel and the Director of Technology, 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 Director of Technology, 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 Acceptable Use Policy & Internet Agreement Policy 712. 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 Director of Technology and the District's business official, shall establish procedures governing management of computer records.

The procedures will address:

- passwords,
- system administration,
- separation of duties,
- remote access,
- encryption,
- 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 Director of Technology, 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 and the District's internal and external auditors. 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
6600, Fiscal Accounting and Reporting
6700, Purchasing
8635, Information Security Breach and Notification

Adoption date: August 21, 2014

POLICY

No. 8630-R

Computer Resources and Data Management Regulation

WESTBURY UNION FREE SCHOOL DISTRICT
BOARD OF EDUCATION

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 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 comprise the network.
- 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 for 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.
- Only those network users with permission from the principal or computer network coordinator may access the District's system from off-site (e.g., from home).
- 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.

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. 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: August 21, 2014

POLICY

No. 8635

Information Security Breach and Notification

WESTBURY UNION FREE SCHOOL DISTRICT
BOARD OF EDUCATION

INFORMATION SECURITY BREACH AND NOTIFICATION

The Board of Education acknowledges the heightened concern regarding the rise in identity theft and the need for secure networks and prompt notification when security breaches occur. To this end, 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. For purposes of this policy, "private information" does not include information that can lawfully be made available to the general public pursuant to federal or state law or regulation;
- 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.

Additionally, pursuant to Labor Law §203-d, the District will not communicate employee "personal identifying information" to the general public. This includes social security number, home address or telephone number, personal electronic email address, Internet identification name or password, parent's surname prior to marriage, or driver's license number. In addition, the District will protect employee social security numbers in that such numbers shall not: be publicly posted or displayed, be printed on any ID badge, card or time card, be placed in files with unrestricted access, or be used for occupational licensing purposes. Employees with access to such information shall be notified of these prohibitions and their obligations.

Any breach of the District's information storage or computerized data which compromises the security, confidentiality, or integrity of personal information maintained by the District shall be promptly reported to the Superintendent and the Board of Education.

Cross-ref: 1120, District Records

5500, Student Records

8630, Computer Resources and Data Management

Ref: State Technology Law §§201-208

Labor Law §203-d

Adoption date: July 17, 2014

POLICY

No. 8635-R

Information Security Breach and Notification Regulation

WESTBURY UNION FREE SCHOOL DISTRICT
BOARD OF EDUCATION

INFORMATION SECURITY BREACH AND NOTIFICATION REGULATION

Definitions

"Private information" shall mean personal information (i.e., information such as name, number, symbol, mark or other identifier which can be used to identify a person) in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- Social security number;
- Driver's license number or non-driver identification card number; or
- Account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account.

"Breach of the security of the system" shall mean 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.

To successfully implement this policy, the District shall inventory its hard copy, computer programs and electronic files to determine the types of personal, private information that is maintained or used by the District, and review the safeguards in effect to secure and protect that information.

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 shall consider:

1. indications that the information is in the physical possession and control of an unauthorized person, such as removal of hard copies, lost or stolen computer, or other device containing information;
2. indications that the information has been downloaded, removed 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.

Security Breaches – Procedures and Methods for Notification

Once it has been determined that a security breach has occurred, the following steps shall be taken:

1. notify those New York State residents whose private information was, or is reasonably believed to have

been acquired by a person without valid authorization. The disclosure to affected individuals shall 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 reasonable integrity of the system.

The District shall consult with the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) to determine the scope of the breach and restoration measures.

2. If the breach involved hard copy or computer data *maintained* by the District, the District shall 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 acquired by a person without valid authorization.

The required notice shall include (a) District contact information, (b) a description of the categories information that were or are reasonably believed to have been acquired without authorization, (c) which specific elements of personal or private information were or are reasonably believed to have been acquired and (d) what the District is doing about it. This notice shall 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, shall 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

Notification of State and Other Agencies

Once notice has been made to affected New York State residents, the District shall notify the State Attorney General, the Department of State Division of Consumer Protection, 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 shall 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.

Adoption date: July 17, 2014