Non-Instructional/Business Operations

SUBJECT: INFORMATION SECURITY BREACH GUIDELINES

The District values the protection of private information of individuals, in accordance with law, regulations, and best practices. The District will work to train staff to prevent breaches, identify breaches, and to take action to rectify the situation should a breach occur. The District is required to notify affected individuals when there has been or is reasonably believed to have been a compromise of the person's private information, in compliance with the Information Security Breach and Notification Act and Board policy.

Definitions

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

2) "Private information" means either:

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

      (1) Social security number;

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

      (3) 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;

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

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

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

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

(Continued)

SUBJECT: INFORMATION SECURITY BREACH GUIDELINES (Cont'd.)

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

All private information stored electronically should be on secure, District-approved information management systems. Employees having access to private information should understand their personal responsibility for protecting student and employee information.

Determining if a Breach Has Occurred

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

1) Indications that the information is in the physical possession and control of an unauthorized person, such as a 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; or

4) System failures.

Recognizing Additional Signs of a Breach

Signs that a computer or system may have been compromised or breached may include the following:

1) Abnormal response time or non-responsiveness;

2) Unexplained lockouts, content, or activity;

3) Locally hosted websites won't open or display inappropriate content or unauthorized changes;

4) Unexpected programs running;

5) Lack of disk space or memory;

(Continued)

SUBJECT: INFORMATION SECURITY BREACH GUIDELINES (Cont'd.)

6) Increased frequency of system crashes;

7) Setting changes;

8) Data appears missing or changed; and

9) Unusual behavior or activity by District staff, students, partners, or other actors.

Employees should report a suspected data breach to the principal or designee and to the Technology Coordinator immediately.

Investigation of Breaches

Breach investigations will be conducted by the District's Technology Coordinator or a designee of the Superintendent. If necessary, law enforcement should be contacted when a breach is detected. Steps to be taken in a breach investigation may include:

1) Determine exactly what information was compromised;

2) Take steps immediately to retrieve data and prevent any further disclosures;

3) Identify all affected records and students and/or employees;

4) Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised;

5) Determine whether institutional policies and procedures were breached, including organizational requirements governing access (usernames, passwords, PINs, etc.); storage; encryption; transmission; and destruction of information from education records;

6) Determine whether the incident occurred because of a lack of monitoring and oversight;

7) Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future;

8) Determine when the breach occurred;

9) Determine which computers or networks were involved;

10) Determine if the data encryption key was compromised;

11) Clarify the scope of the breach and the individuals involved;

(Continued)

SUBJECT: INFORMATION SECURITY BREACH GUIDELINES (Cont'd.)

12) Determine if the breach also involved additional cyber incidents such as denial of service, scans or malicious code.

The District should utilize a back-up system to ensure continuity of operations.

Notification Requirements

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

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

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

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

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

(Continued)

SUBJECT: INFORMATION SECURITY BREACH GUIDELINES (Cont'd.)

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

Methods of Notification

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

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 a log of each notification is kept by the District when notifying affected persons in electronic form. However, in no case will the District require a person to consent to accepting the notice in electronic form as a condition of establishing any business relationship or engaging in any transaction;

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

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

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

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

    c. Notification to major statewide media.

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

1) Contact information for the notifying District;

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

(Continued)

SUBJECT: INFORMATION SECURITY BREACH GUIDELINES (Cont'd.)

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

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

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

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

State Technology Law §§ 202 and 208