Non-Instructional/Business Operations

MOUNT PLEASANT COTTAGE SCHOOL UNION FREE SCHOOL DISTRICT

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 such 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 (State Technology Law Section 208) and Board policy.

Definitions

"*Private information*" shall mean "*personal information*" 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:

1) Social security number;

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

3) 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.

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

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

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

(Continued)

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

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; or

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

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 account lockouts;

3) Inoperable passwords;

4) Inability to open website homepage or unexplained changes/content to website;

5) Programs not running properly;

6) Lack of disk space or memory;

7) Bounced back emails;

8) Inability to connect to the network;

9) Continuous or increasing crashes;

10) Abnormal hard drive activity;

(Continued)

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

11) Connecting to unfamiliar sites;

12) Changes in browser settings;

13) Extra or unfamiliar toolbars that cannot be deleted.

Employees should report a suspected data breach to the Principal and/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 (i.e., names, addresses, contact information, social security numbers, student or employee ID numbers, credit/debit card numbers, grades, birth dates, passwords);

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 (user names, 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;

(Continued)

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

11) Clarify the scope of the breach and the individuals involved (i.e., did it affect a specific, identifiable group of individuals on the District's network or was it random);

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

The District will notify the New York State Attorney General (AG), the New York State Division of Consumer Protection and the New York State Office of Cyber Security (OCS), as required by law. All affected individuals must be notified of the breach if their compromised data meets the classifications described in law. The District may delay notification of affected individuals if law enforcement determines that notification may impede a criminal investigation.

The required notice shall 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 such notification is kept by the District when notifying affected persons in electronic form. However, in no case shall the District require a person to consent to accepting such 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 such notification is kept by the District when notifying affected persons by phone; or

4) Substitute notice, if the District demonstrates to the 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 shall consist of **all** of the following:

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

(Continued)

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

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 of which notice is provided, a notification must include:

1) Contact information for the District official handling the notification;

2) A description of the categories of information that were, or are reasonably believed to have been, acquired without authorization; and

3) Details on which elements of personal and private information were, or are reasonably believed to have been, so acquired.

The New York State Office of Cyber Security will be informed as to the timing, content and distribution of the notices and the approximate number of affected persons. The Attorney General and the Division of Consumer Protection should also be informed of these notices to affected persons. Refer to Form #5672F -- New York State Security Breach Reporting Form for contact information, addresses and notification guidelines.